ISSN : 2347 - 8446 (Online)
ISSN : 2347 - 9817 (Print)

A Progress of Next Generation Network

[I]M.Buvaneswari, [II]Dr.N.Rajendran
[I]Research Scholar, Bharathiar University, Coimbatore, Tamilnadu, India.
[II]Principal, Vivekanandha Arts and Science College for Women, Sankari, Tamilnadu, India

Abstract
A Next Generation Networking (NGN) is a Packet based and IP based network that used to transmit all kinds of services and information including voice data/calls, audio data/calls and multimedia information such as videos. It provides services like broadband, telecommunication and is also able to use QoS. Security protection is part of NGN service management via IP protocols. The use of IP protocols as the foundation of NGNs gives great flexibility, but also exposes the networks to all the security threats found on the Internet. NGNs do not have a strong separation between signaling and control channels, and the payload channels. Denial of service attacks, toll fraud, information theft, and user privacy threats are real in NGNs. We present an overview of the NGN with its basic architecture and discussion about IPv6 Protocols.

Keywords
Next Generation Network, Packet-based Network, Securities, IP Protocols

I. Introduction

The NGN is a wide model covering a variety of network types from wired to wireless, and from telecommunication to computer. It was designed to use a common network protocol to carry all data/service/application which may be carried by different data/service/application-specified networks currently over a common and open network infrastructure. ITU-T defines the NGN as follows [1]:

"The NGN is a packet-based network able to provide Telecommunication Services to users and able to make use of multiple broadband, QoS-enabled transport technologies and in which service-related functions are independent of the underlying transport-related technologies. It enables unfettered access for users to networks and to competing service providers and services of their choice. It supports generalized mobility which will allow consistent and ubiquitous provision of services to users." (ITU-T, 2004)

NGNs provide a rich range of IP-based services for telecommunications operators, including voice, data, video, TV and messaging. NGN originates from the telecommunication industry and standardization organizations like ETSI, ITU-T and 3GPP. Traditional telecommunication's are throwing out SS7 signaling (Signaling System #7) and various SDH hierarchies for transport (Synchronous Digital Hierarchy), and replace those by all-IP networks with a standardized service control platform called IP Multimedia Subsystem (IMS).

Furthermore, in order to deliver those services to end-users effectively and efficiently, a variety of broadband technologies are supported by an NGN as well. An NGN also offers possibilities for customers to customize their services in a flexible way. The NGN is also capable of generalizing mobility and converging services between mobile and stationary devices, retain compatibility with legacy systems, and allow users to select service providers unrestrictedly.

NGN offers several advantages at various levels of services [2].

- **Unified Messaging,** it supports the transmission of voice mail, email, fax mail, and pages through common interfaces.
- **Data Connectivity,** it offers many value added services such as bandwidth on demand, durable Switched Virtual Connections (SVC), call admission control etc.
- **Voice Telephony,** it supports all traditional telephony services besides focusing on the most marketable voice telephony features.
- **Multimedia,** it enables collaborative computing and groupware and supports interactivity among multiple parties sharing voice, video, and/or data.
- **Public Network Computing (PNC),** it supports generic processing and storage capabilities, Enterprise Resource Planning (ERP), time reporting, and miscellaneous consumer applications.
- **Home Networking,** it supports intelligent appliances, home security systems, energy systems, and entertainment systems.
- **Virtual Call Centers,** it enables voice calls and e-mail messages through queue system, electronic access to customer, catalog, stock, and ordering information, and communication between customer and agent.
- **Information Brokering,** it offers advertising and information delivery based on pre-specified criteria or personal preferences and behavior patterns.
- **Interactive Gaming,** it establishes interactive gaming sessions among multiple users.
- **Virtual Private Network (VPN),** it offers uniform dialing capabilities for voice VPNs and added security and network features for data VPNs.
- **Ecommerce,** it enables e-transactions, verification of payment information, trading, home banking and shopping etc.
- **Distributed Virtual Reality,** it builds up co-ordination among multiple diverse resources in providing real world events, people, places, experiences, etc.

II. Next generation core networks:

The next generation core networks are defined on the basis of their underlying technological "components" that include – as mentioned in the ITU definition – packet-based networks, with the service layer separated by the transport layer, which transforms them into a platform of converged infrastructure for a range of previously distinct networks and related services. These features may have an impact on traditional business models and market structure, as well as on regulation:

IP-based network: "Next generation core networks" generally cover the migration from multiple legacy core networks to IP-based networks for the provision of all services. This means that all information is transmitted via packets. Packets can take different routes to the same destination, and therefore do not require the establishment of an end-to-end dedicated path as is the case for PSTN-based communications.

Packet-based, multi-purpose: While traditionally separate networks are used to provide voice, data and video applications, each requiring separate access devices, with NGN different kinds of applications can be transformed into packets, labeled accordingly and delivered simultaneously over a number of different transport technologies, allowing a shift from single-purpose networks (one network, one service), to multi-purpose networks (one network, many services). Interworking between the NGN and existing networks such as PSTN, ISDN, cable, and mobile networks can be provided by means of media gateways.

Separation of transport and service layer: This constitutes the key common factor between NGN and convergence, bringing about the radical change in relationship between network "layers" (transport infrastructure, transport services and control, content services and applications). In next generation networks service-related functions are independent from underlying transport-related technologies (Figure 1). The uncoupling of applications and networks allow applications to be defined directly at the service level and provided seamlessly over different platforms, allowing for market entry by multiple service providers on a non-discriminatory basis [3].

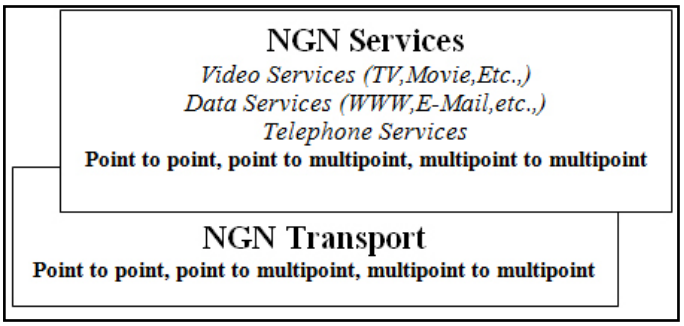

Fig.1: Functional planes

In addition, the deployment of wireless infrastructures facilitates access to IP networks, and the adoption of increasingly sophisticated devices and handsets will allow an easy access to IP services from anywhere. The migration process towards IP-NGN potentially entails several structural changes in the core network topology, such as the rearrangement of core network nodes and changes in the number of network hierarchy levels. As a result, an overall reduction in the number of points of interconnection will take place, especially with regard to interconnection points at the lowest level.

Although the shift in the migration to all-IP networks is taking place at different paces in different countries, several operators in the OECD area have already updated their transport networks, and are now dealing with NGN at the local access level. Solutions embraced by fixed operators may also increasingly support IP Multimedia Subsystem (IMS), to enable fixed-mobile convergence [4].

For the moment the most common services provided through the new networks are the provision of PSTN/ISDN emulation services, i.e. the provision of PSTN/ISDN service capabilities and interfaces using adaptation to an IP infrastructure, and video on demand (VoDs). At the same time the business world is showing an increasing interest in new NGN-enabled services and applications. Companies are migrating their Time Division Multiplexing switches to IP in order to enable integrated applications for specific industry-based functionalities and purposes [5].

Progress in the field of mobile (cellular) communications is taking shape with the development of the IMS standard. For the moment two services have been standardised under the IMS protocol, Push to Talk over Cellular (PoC) and Video Sharing. Prominent telecommunication network equipment suppliers are actively supporting the take up of IMS and some of them are implementing IMS strategies and commercial IMS products [6][7]. IMS is seen as the enabler for the migration to next generation networks of mobile operators and therefore for the implementation of fixed-mobile convergence. No evident killer application has currently emerged, with many operators focusing on one specific service: voice. Facilitating the use of voice applications, enabling users to handle their calls easily between fixed and mobile networks, and to receive calls wherever they are, is fundamental for the take–up of the service. Operating in an IMS environment would allow a seamless handover from WLAN (fixed) to mobile during calls (Voice Call Continuity). In order for real-time voice calls to be offered seamlessly between the circuit switched domain and the Wireless LAN interworking with IMS architecture, the Third Generation Partnership Project (3GPP) [8] is currently working to develop the appropriate Technical Specifications to define this functionality as a standard 3GPP feature. The study by 3GPP of the standard is underway. In the meanwhile, fixed-mobile converged services have been launched by some mobile operators with access to fixed networks, using a different standard – Unlicensed Mobile Access (UMA) – allowing users to seamlessly switch from fixed to mobile networks.

In addition, increasing competitive pressure on mobile carriers is coming from the IP world. Thanks to the availability of dual-use devices and Wi-Fi hotspots, service providers – such as Skype, Google, and others – are able to offer on the market a host of new services for mobile users in a very short period of time. This rapidity constitutes an important comparative advantage, which in some cases provoke the reaction of mobile operators (and manufacturers), tending to limit the services and applications users can access from their mobile handset [9] [10].

III. Next Generation Network Architecture:

It is a universal multi-service network designed (Figure 2) for the transmission of voice, images and data on a packet switching basis. An NGN provides the quality of service necessary or different types of telecommunication traffic. Characteristically, the transmission and the routing of the packets and the elements of the transmission equipment (links, routers, switches and gateways) are physically and logically separated from the devices and the intelligence controlling the execution of calls and services. The network intelligence supports all types of services in the packet network, from basic voice telephony to data, image, multimedia, broadband and management applications. NGN Architecture is based on four functional layers: User Access Layer, Application and Service Layer, Transport Layer and Control Layer [1].

ISSN : 2347 - 8446 (Online)
ISSN : 2347 - 9817 (Print)

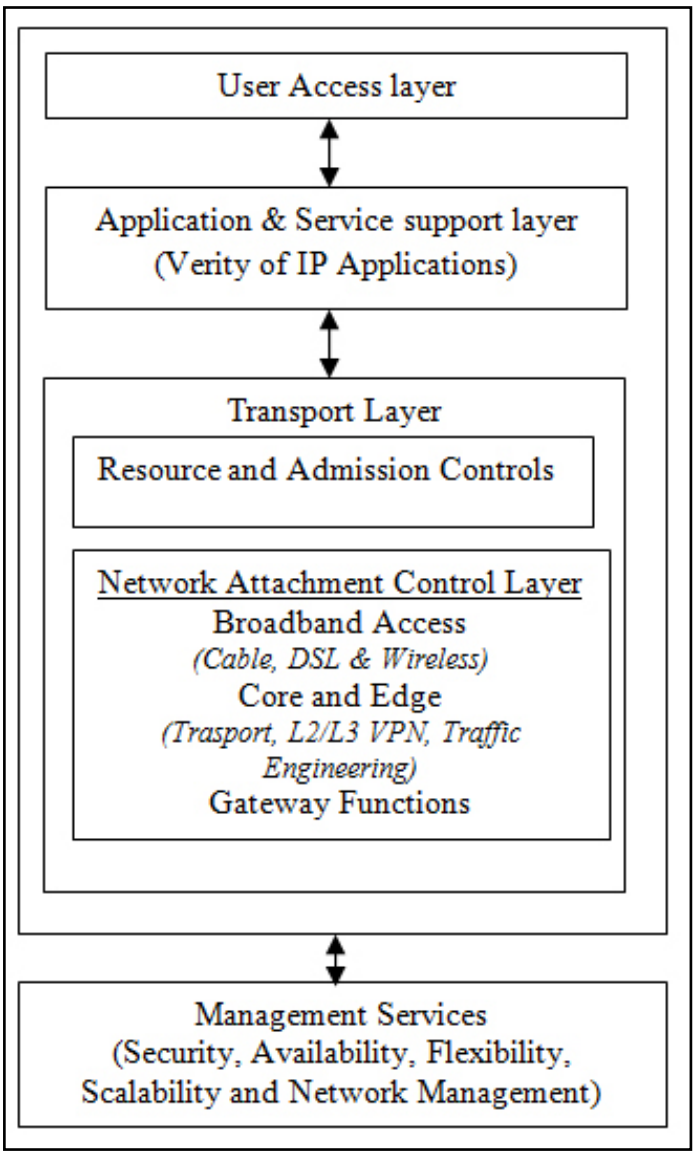

Fig. 2: NGN Architecture

User Access Layer: It is the lowest layer in the model. It supports infrastructure for access of end user devices, like wireless or standard telephones, mobile or desktop computer etc., to transport network and vice versa. Physical interconnection can be realized with different type of transport mediums from standard telephone loopback, fiber, xDSL technologies to FWA.

Application and Service Layer : It is also common to call it a service layer, because it merger so called application servers and a media servers (platforms for diffusions of content). Web services inspired by internet and by distributed intelligence services based on functions of servers in management layer with centralized intelligence Services offered in network mediums of other operators. Service layer provides basic blocks of services, from which operators can make their more complex and more usable service. Examples are function blocks bounded on: transmission and routing (for example establishment of channel in network, routing of communication, limiting of communication to selected networks, QoS and others). Communication and provision of informative content (voice management or multimedia communication, limiting of access to selected types of services, locating of geographic position of user, determination of connection status of user…). Access and billing (autentification of user, gathering of information about usage of network by that user, bill issuing…).

Transport Layer : The transfer of data including the control and management information for data transfer is accomplished by this function block. This Layer includes: Access Network Functions, Edge Functions, Core Transport Functions and Gateway Functions. It is consisting from one or from multiple high-speed backbone packet switched networks. It is possible to serve to a flows of different character with different requirements on quality of transfer (delay, data loss,...). On interface in direction to access networks and to networks of another operators are mediation gateways (MGW) situated, which are adapting and routing data flows between these networks and unified transport network. Elements of Signaling gateway (SGW) are converting inherent signalization. Unified shared version of IP protocol can cooperate with GMPLS interconnection[11].

Control and Network Layer : The Network Attachment Control layers which are required for registration and initialization of end user services in access network, and Resource and Admission Control functions which are required for QoS, Network Address and Protocol Translation (NAPT) and firewall traversal control support. Management layer is to control other layers. It is liable for correct functioning of management of transport layer (MGW/SGW). It controls service calling (application layer) and also manages user profiles (user access layer). One of the main principles of NGN architecture is it's division of management functions from connection hardware. In traditional telephony, connection functions of transport layer and functions of management layer were supported by one device - exchange. In NGN, elements MGW/SGW are used as connection and routing function of exchange (switching network, interface and signaling). Servers for controlling of calling (Soft switch) are replacing controlling functions of exchange (processors and memories). This division with use of packet network, primarily for data transfers, is used also for voice and multimedia communication in real time [1].

Here, uses the network protocols IP and MPLS with the optical fiber transport technology ASON/OTN to build up their core NGN transport networks.

More importantly, a basic element of the NGN concept, the network protocol, is not explicitly specified in the ITU-T's recommendations released so far, in other words, theoretically it may be any protocols once they are able to meet the NGN requirements. However, currently a industry-wide consensus has been achieved whereby the Internet Protocol (IP) is considered as the most appropriate solution to establish connectivity for all network equipments and carry data/services/applications both inside (NEs) and outside (end-user terminals) an NGN.

This is mainly because IP is now indeed predominant in the network world and widely considered as the most promising technology to build up an NGN. Thus, the main idea of NGN can be finally described as "IP over everything" and "Everything over IP" [12], where IP packets are used to carry all types of data over all transport mediums (optical fibre, copper line, or radio wave) across all sub-networks within an NGN. With this idea, all existing telecommunication networks and the Internet will converge into a unified IP-based packet-switching network infrastructure ultimately, and therefore NGN should be able to benefit from both the worlds of conventional telephone networks (PSTN/ISDN) and the Internet.

NGN requirements could label themselves as NGN; some industry-wide accepted and practice-proved core NGN technologies are listed below:

Soft-switch: NGN provides PSTN/ISDN emulation and simulation services, which are used to enable end-users to use their legacy terminals with NGN continuously and have similar experience to the legacy system in an NGN environment. In conventional PSIN/ ISDN systems, switches or switchboards are used to control calls, similarly, a programmable device called soft-switch or call-sever in an NGN is used to control Voice over IP (VoIP) calls, and allow users to use the legacy telephone numbering system. Soft-switch in NGN is also used to establish the interface to co-operate with the legacy PSTN/ISDN, through SG (Signaling Gateways) and MG (Media Gateways) technology [13].

MPLS (Multi-Protocol Label Switching): MPLS and its subsequent development (Generalized Multi-Protocol Label Switching or GMPLS for short) are virtual circuit switching protocols, and were designed to carry data for both circuit switching nodes and packet switching nodes. MPLS is an important element enabling NGN services by providing IP based networks with basic traffic engineering ability such as CoS (Class of Service) and packet priority [14]. It is noted that MPLS has to work in conjunction with IP within an NGN environment.

Core Transport Technology: IP over ASON over OTN: Wavelength Division Multiplexing (WDM) technology is widely used in the telecommunication backbone/core transport networks to provide solid transport services due to its tremendous line rates. The next generation optical transport technology based on WDM is developed and named Optical Transport Network (OTN). Automatically Switched Optical Network (ASON) is an independent control plane added on OTN to gain more control and management advantages. Furthermore, IP is the virtually dominant network protocol now in the world to carry a variety of services and applications [15].

IV. The NGN Network Protocol (IPv6)

Internet Protocol version 6, or IPv6 for short, is a later version of IP suite; it is selected as the primary network protocol for the NGN. The transition to IPv6 is usually considered important as the Internet will run out of its IPv4 addresses in the next decade, and IPv6 can provide many more potential addresses (2128 vs. 232). But the improved overall performance of the IPv6 Internet, including higher network throughput, enhanced QoS and etc, is also significant [16] .

IPv6 has been developed for over a decade; its development was initiated in early 1990 by IETF (the Internet Engineering Task Force) to "*address perceived scaling problems in the Internet's addressing and routing architectures*" (Nightingale, 2007). Now it has been widely accepted and deployed in the telecommunication industry, its commercial implementations are emerging on a large scale to replace its previous version.

In detail, IPv6 implementation is required as it is designed to meet the demand of the industry to handle the increasing number of Internet applications. Firstly, by the year 2010, the number of PC users is expected to grow to more than one billion; the rapid growth of the PC market stimulates demands on the Internet capacity: more IP addresses are needed. Secondly, the non-PC electronic devices with network capability, such as PDA and smart phone, are also expected to show a rapid growth in the next few years. Furthermore, the entertainment business also accelerates this transition process, more and more online entertainments, such as online music, video stores, and online gaming, require higher capacity of the Internet. In addition to the above, the rapidly increasing online communications, including instant messenger, email and etc, also result in intense demands on the Internet capacity [17].

From a technical perspective, as a part of NGN, IPv6 emphasizes some important technical updates to cover the shortcomings of its previous version IPv4. In detail, one of the most significant changes while moving to IPv6 from IPv4 is the improved IP address length, from a 32-bit length in IPv4 to 128-bit long in IPv6. At present, 4,294,967,296 (232) unique addresses provided by IPv4 are almost running out due to the increased number of internet applications and inefficient resource allocation. For example, in 2008, the IPv4 addresses assigned for China were reported to be used up to 80%, and would run out in 830 days (Thompson, 2008). However, IPv6 can provide340,282,366,920,938,463,463,374,607,431,768,211,456 (2128) unique addresses, which are almost infinite for us in the coming decade.

Moreover, IPv6 improves the overall throughput of the next generation IP networks by supporting a Jumbo grams mode in packet encapsulation, and it provides much larger single packet size (Maximum Transport Unit or MTU for short) than IPv4, where packets are limited to 64k, IPv6 breaks this limit and supports MTU up to 4GiB. Thus, some upper applications can gain significant performance improvement on data transfer by using larger MTU within IPv6 networks.

IPv6 developers also redesigned the IPv6 routing architecture by adopting a simplified fixed-length header structure and a more rational fragmentation mechanism, to enable faster header processing at intermediate routers and improve packet forwarding performance, consequently to enhance the overall network throughput. The checksum packet header field used for error checking in IPv4 is no longer used in IPv6 in order to avoid extra overhead caused by re-computing the checksum in intermediate routers. Instead, the error checking is performed in a lower layer by transport protocols. In addition, packet fragmentation is also no longer performed by routers in IPv6 networks; it is performed by the communication end points instead in order to improve the overall network performance.

More important, IPv6 significantly enhances its QoS performance by adopting a traffic class field and a flow label field in packet header to replace "service type" which is used in IPv4 for routers to configure packets' priorities. In terms of security, the adoption of IPSec in IPv6 can provide end-to-end security guarantee for upper protocols or services/applications, and the enhanced security in a router level. Besides the above, IPv6 integrates a set of security mechanisms such as IP encryption and authentication by mandatorily supporting these security mechanisms in IPv6 packet header. In contrast, those security mechanisms are optional in IPv4.

In addition, IPv6 supports "plug and play", and mobility. In IPv6 networks, the network hosts can automatically assign themselves IP address or necessary configuration parameters by sending router discovery messages (a link-local multicast router solicitation request) to and receiving replies (a router advertisement packet) from routers when connecting to the network. This advanced feature simplifies the network management, and is relatively easy for supporting mobile nodes. In addition, IPv6 mobile suit (Mobile IPv6 or MIPv6 for short) defines some new features dedicated for mobility to allow it to work as efficiently as normal IPv6. Finally, IPv6 introduces a concept of multicast scoping and labelling, which is used to limit the routing scale for multicasting and identify permanent and temporary addresses [18].

When moving towards a new technology, the transition process is always important to the final success, just like other NGN deployments, the transition from IPv4 to IPv6 is a long term and

ISSN : 2347 - 8446 (Online)
ISSN : 2347 - 9817 (Print)

stepwise process. Until IPv6 hosts completely supplant IPv4 ones, a number of so-called transition mechanisms are required to enable the intercommunication between IPv6 and IPv4 nodes. These mechanisms, collectively called SIT (Simple Internet Transition) techniques, include:

Dual-Stack IP: it was designed to provide communication abilities between an IPv6 and an IPv4 node, with this approach, the network nodes have both IPv4 and Ipv6 stacks for supporting intercommunications between IPv6 and IPv4 nodes. This approach is generally considered relatively easy but increases the system complexity.

NAT-PT: Network Address Translator (NAT) or Protocol Translator (PT) makes communications among non-homogeneous networks possible by providing application-agnostic network address or protocol translation services at the IP layer.

Dual stack IP ALG: the dual stack IP ALG (Application Layer Gateway) proxies running on the network borders can provide protocol translation services at the application layer to enable communications between IPv4 and IPv6 networks.

IPv6-over-IPv4 Tunnelling: it was designed to provide the communication between two IPv6 nodes over an IPv4 network; this tunnelling technique uses IPv4 as a link layer for IPv6 through encapsulating IPv6 packets into IPv4 form so the IPv6 packets can be transmitted over the IPv4 networks [19].

V. IPv6 Security Issues

The transition from IPv4 to IPv6 is under way as more network and content providers embrace IPv6. As the amount of IPv6 traffic (and IPv6-based threats) increases in your network, it's essential that you deploy a network security solution that can deliver the same level of protection for IPv6 content as IPv4. Organizations of all sizes need to understand the security implications of IPv6, which include [20]:

IPv4 security devices cannot inspect IPv6 traffic Although there are work-around measures to enable IPv4 network and security devices to forward IPv6 packets, IPv4 devices cannot inspect those packets for malicious content. This lack of visibility enables a simple evasion technique to avoid detection by legacy security devices--send malicious content via IPv6. This allows old threats to bypass policies that may have been in place for years. And, as long as the victim system can process IPv6, the attack will reach its intended target.

IPv6 is likely in your network today, as many systems (such as Windows 7) natively support IPv6 and ship with IPv6 support enabled Many systems ship today with IPv6 support enabled by default. And, unless that support is specifically disabled, these devices will be vulnerable to threats transported via IPv6.

Some legacy security devices will never support IPv6 and will need to be replaced Many network security devices require recently released versions of their operating systems to support IPv6. Unfortunately, not all devices can support the most recent releases due to lack of memory or other hardware-based limitations, requiring an upgrade to the latest hardware device. Without replacing the device, the network segments protected by these legacy systems will be blind to threats embedded within IPv6 traffic.

Many security vendors have limited support for IPv6 today, leading to potential gaps in protection Supporting IPv6 with a dual-stack architecture is not a trivial development exercise; it requires a significant allocation of development resources to build a new stack and incorporate it with the existing IPv4 stack. Many vendors have only recently committed development resources to supporting IPv4, choosing to wait until demand for IPv6 support increased before allocating the necessary resources. One result of the delayed investment is that they will not be able to offer feature parity with their IPv4 devices, which has the potential to lead to years of gaps in IPv6 policy enforcement, as these vendors will struggle to make all key IPv4 features functional in IPv6.

IPv6 support is often at much slower performance In addition to reduced functionality in their IPv6 support, many vendors rely on software only to filter traffic to detect threats. As stated above, the implementation of IPv6 support in a network security device is not a trivial exercise. It requires significant investment and, like any other new technology, several product releases to deliver stable, mature functionality. One way to accelerate the speed with which they can bring IPv6 support to market, vendors of devices that utilize custom processors will release IPv6 support in software only. The advantage is that a software-only approach reduces the amount engineering effort required to bring the functionality to market. The disadvantage is that the performance of a software-only approach is significantly slower than a hardware-accelerated approach.

VI. Conclusion

Next-generation networks must be flexible enough to support IPv6 Securities. In order to maintain high throughput and reliability, these complex networks must have security devices that won't become chokepoints as they inspect and filter traffic for threats and malware. In order to protect next-generation networks against both known and new threats, these security devices must be based on field-proven, highly-scalable, and easy-to-manage platforms.

Reference

[1]. ITU-T. (2004). ITU-T Recommendation Y.2001: General overview of NGN. Retrieved December 2, 2008, from http://www.itu.int/itudoc/itu- t/aap/sg13aap/history/y2001/y2001.html

[2] Lakshmi, "Next generation Network", http://ipv6.com/articles/general/Next-Generation-Networking.htm

[3] Keith Knightson, Industry Canada, ITU NGN Architecture, presentation at the "ITU-IETF Workshop on NGN", May 2005, Geneva

*[4] IMS is an architectural framework for delivering *Internet protocol (IP) multimedia services to mobile users, aiding the access of multimedia and voice applications across wireless and wireline terminals, and therefore foster fixed mobile convergence (FMC). Initially developed in the framework of the Third Generation Partnership Project (3GPP), IMS Release 7 was developed in co–operation with ETSI TISPAN, in order to support fixed networks. See http://www.etsi.org/tispan/. S. Pileri, Telecom Italia, presentation at the meeting with the financial community (2007); British Telecom, with its 21st Century Network project; France Telecom announced its plans to introduce IMS in its networks starting from 2007, etc.*

[5] Alessandro Rossi, Italtel, phone interview, March 2007. "Technical progress, market evolution and the regulation of the electronic communications sector in the EU", Paul Richards, BT.

[6] The IP Multimedia Subsystem (IMS) was originally developed for 3rd generation networks and is now considered the standard for fixed and mobile IP-based communication by mobile operators.

[7] See for example Ericsson IMS products description at http://

www.ericsson.com/products, or Nokia IMS at http://www.nokia.com/A4126030.

[8] The 3rd Generation Partnership Project (3GPP) brings together a number of telecommunications standards bodies which include ARIB, CCSA, ETSI, ATIS, TTA, and TTC. See the 3GPP website online at http://www.3gpp.org.

[9] 3GPP Active Work Programme, Voice call continuity (VCC) between CS and IMS (incl. I-WLAN), online at http://www.3gpp.org/ftp/Specs/html-info/FeatureOrStudyItemFile-32091.htm.

[10] Unlicensed Mobile Access (UMA), is the 3rd Generation Partnership Project (3GPP) global standard for subscriber access to mobile circuit, packet and IMS-based services over any IP-based access network, including the Internet. UMA allows seamless roaming and handover between local area networks and wide area networks using a dual-mode mobile phone. See http://www.umatoday.com/umaOverview.php.

[11] NGN Architecture : http://ngnlab.eu/index.php/ngn-knowledgebase/ngn-architecture

[12] Crimi, J. C. (2005). Next Generation Network (NGN) Services. Retrieved December 2, 2008, from http://www.mobilein.com/NGN_Svcs_WP.pdf

[13]. Gou, X., Jin, W., & Zhao, D. (2004). Multi-agent Based Softswitch. Proceedings of Intelligent Agent Technology 2004 (IAT 2004), 341 – 344.

[14]. Kang, Y., & Lee, J. (2005). The implementation of the premium services for MPLS IP VPNs. Proceedings of the 7th International Conference on Advanced Communication Technology 2005, 2, 1107 – 1110.

[15]. Lee, C., & Morita, N. (2006). Next Generation Network Standards in ITU-T. Broadband Convergence Networks, 2006. Proceedings of the 1st International Workshop 2006, 1 – 15.

[16] Bradner, S., & Mankin, A. (1995). The Recommendation for the IP Next Generation Protocol (IETF RFC1752). Retrieved December 2, 2008, from http://tools.ietf.org/html/rfc1752

[17] Dubey M. P. (2005). Implementation of IPv6: The Next Generation Internet. Retrieved December 2, 2008, from http://searchwarp.com/swa5844.htm

[18] Bradner, S., & Mankin, A. (1995). The Recommendation for the IP Next Generation Protocol (IETF RFC1752). Retrieved December 2, 2008, from http://tools.ietf.org/html/rfc1752

[19] Gilligan, R., & Nordmark, E. (1996). RFC1933 - Transition Mechanisms for IPv6 Hosts and Routers. Retrieved December 2, 2008, from http://tools.ietf.org/html/rfc1933

[20] Fortinet ,IPv6 and Fortinet Solution Guide - IPv6: Network Security and the Next Generation of IP Communication

Authors Profile

M.Buvaneswari received her M.Phil (C.S) Degree from Bharathiar University, Coimbatore in the year 2006. She has received her M.Sc.,(CS) Degree from Periyar University, Salem in the year 2004. She is working as Assistant Professor, Department of Computer Science, Vivekanandha College for Women, Namakkal, Tamilnadu, India. She's areas of interest include Data Communication and Network, Network Security and Wireless

Dr. N.Rajendran received his Ph.D Degree from Periyar University, Salem in the year 2011. He has received his M.Phil, Degree from Bharathiar University, Coimbatore in the year 2000. He has received his M.C.A Degree from Madras University, Chennai in the year 1990. He is working as Principal of Vivekanandha Arts and Science College for Women, Sankari, Salem , Tamilnadu, . He has 23 years of experience in academic field. He has published 8 International Journal papers and 13 papers in National and International Conferences. His areas of interest include Digital Image Processing and Networking.