The Impact of IPv6 on Video-to-Video and Mobile Video Communications

Latif Ladid[1] and Ioannis P. Chochliouros[2]

[1] President, IPv6 Forum & Senior Researcher, Snt, University of Luxembourg,
6, Rue Richard Coudenhove-Kallergi, L-1359 Luxembourg-Kirchberg, Luxembourg
latif@ladid.lu
[2] Research Programs Section,
Hellenic Telecommunications Organization (OTE) S.A.,
99 Kifissias Avenue, GR-151 24, Athens, Greece
ichochliouros@oteresearch.gr

Abstract. New technologies, viewing paradigms and content distribution approaches are about to take the TV/video services industry by storm. Five emerging trends are observable, *among which is the worldwide deployment of IP Version 6 (IPv6),* that are all related to the next-generation delivery of entertainment-quality video and can be capitalized upon by progressive service providers, telcos, cable operators, and ISPs. This work aims at exploring the IPv6-based evolving trends and offering practical suggestions of how it could support effective growth of video-to-video and mobile video communications. It also addresses an overview of IPv6; the rapid expansion of video-based solutions in the ICT market sector; IPv6 advantages for enhanced video communications as well as QoS issues from the use of IPv6 and IPv6 multicast approaches.

Keywords: Data services, Internet, Internet Protocol (IP), internetworking, IPv6, mobility, multimedia, Quality of Service (QoS), video, web services.

1 Introduction: IPv6 Basics

Internet Protocol (IP) version 6 (IPv6) is a newer version of the network layer protocol that is designed to coexist with IPv4 and, *eventually*, replace it. It provides improved internetworking capabilities compared to what is presently available with IPv4 [1]. The current IPv4 version of the IP has been in use for 30 years but it exhibits some challenges in supporting emerging demands for address space cardinality, high-density mobility, multimedia and strong security. IPv6 offers the potential of achieving scalability, reachability, end-to-end interworking, Quality of Service (QoS), and commercial-grade robustness that is needed for contemporary and emerging web services, data services, and IP-based TV (IPTV)/IBTV/NTTV content distribution. The innovation and growth of the Internet is now predicated on deployment of IPv6 where the latter is not strictly and uniquely required to support IP-based IBTV/NTTV/IPTV, linear video, Video/Content On-Demand (VoD/CoD), and/or

L. Iliadis et al. (Eds.): AIAI 2012 Workshops, IFIP AICT 382, pp. 322–331, 2012.

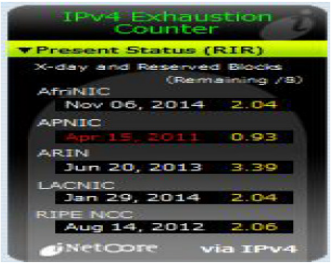
streaming video, just that it provides an ideal, future-proof, scalable mechanism for such services, whether in a terrestrial mode on in a satellite-based mode.

IP was designed in the late 1970s- early 1980s for the purpose of connecting computers that were in separate geographic locations. Starting in the early 1990s, developers realized that the communication needs of the 21st century required a protocol with some new features and capabilities while, *at the same time,* retaining the useful features of the existing protocol. Like IPv4, IPv6 is an Internet-layer protocol for packet-switched interworkings and provides end-to-end datagram transmission across multiple IP networks. IPv6 [2] was initially developed in the early 1990s because of the anticipated need for more end-system addresses based on anticipated Internet growth [3], encompassing mobile phone deployment, smart home appliances, and billions of new users in developing countries (e.g., BRIC: Brazil, Russia, India, China). Technologies and applications such as Voice-Over-IP (VoIP), "always-on access" (e.g., cable modems), broadband and/or Ethernet-to-the-home, converged networks, and evolving ubiquitous computing applications will be driving this need even more in the next few years. IPv6 is now being slowly deployed worldwide: there is documented institutional and commercial interest and activity in Europe and Asia, and there also is evolving interest in the U.S. [4]. The expectation is that in the next few years, deployment of this new protocol will occur worldwide. For example, the U.S. Department of Defense (DoD) announced that from *May 2012*, all procurements needed to be IPv6-capable; the DoD's goal was to complete the transition to IPv6 for all intra- and inter- networking across the agency by *2013*, which was accomplished. The U.S. Government Accountability Office (GAO) has recommended that all agencies become proactive in planning a coherent transition to IPv6. The current expectation is that IPv4 will continue to exist for the foreseeable future, while IPv6 will be used for new broad-scale applications [5]. The two protocols are not directly interworkable, but tunneling and dual-stack techniques allow co-existence and co-working as well.

While the basic function of the network layer internetworking protocol is to move information across networks, IPv6 has more capabilities built into its foundation than IPv4. Link-level communication does not generally require a node identifier (address) since the device in intrinsically identified with the link level address; however, communication over a group of links (i.e., a network) does require unique node identifiers (addresses). The IP address is an identifier that is applied to each device connected to an IP network. In this setup, different entities taking part in the network (servers, routers, user computers, and so on) communicate among each other using their IP address, as an entity identifier. The current IPv4 naming scheme was developed in the 1970s and had capacity for about 4.3 billion addresses, which were grouped into 255 blocks of 16 million addresses, each. In version 4 of the IP protocol, addresses consist of four octets. With IPv4, the 32-bit address can be represented as: *AdrClass*|*netID*|*hostID*. The network portion can contain either a network ID or a network ID and a subnet. Every network & every host (or device) has a unique address, *by definition*. For ease of human conversation, IP protocol addresses are represented as separated by periods, for example: 166.74.110.83, where the decimal numbers are a short hand (and correspond to) the binary code described by the byte in question (an 8 bit number takes a value in the 0-255 range). Since the IPv4 address

has 32 bits there are nominally 2^{32} different IP addresses (as noted, approximately 4.3 billion nodes, if all combinations are used). This expansion allows for many more devices and users on the Internet as well as extra flexibility in allocating addresses and efficiency for routing traffic. It also eliminates the primary need for network address translation (NAT), which gained widespread deployment as an effort to alleviate IPv4 address exhaustion. The vast additional address space available with IPv6 can help the Internet to support the next generation of wireless, high-bandwidth, multimedia applications as well as growth in the overall number of users [6].

IPv4 has proven, by means of its long life, to be a flexible and powerful networking mechanism. However, IPv4 is starting to exhibit limitations, not only with respect to the need for an increase of the IP address space, driven, *for example:* by new populations of users in countries such as China and India; by new technologies with "always connected devices" (e.g., cable modems, networked PDAs, 3G/4G mobile smart-phones, and so on), and; by new services such global rollout of VoIP, IPTV, and social networking. A Regional Internet Registry (RIR) manages the allocation & registration of Internet resources such as IPv4 addresses, IPv6 addresses and Autonomous System (AS) Numbers, in a specific region of the world. As of *February 1, 2011* only 1 percent of all possible IPv4 addresses were left unassigned. This has led to a predicament known as the "*IPv4 Run-Out"*. The entire address space was expected to be more or less exhausted by *August 2012* in Europe (Fig.1).



RIR = Regional Internet Registry
AfriNIC = African Network Information Centre
ARIN = American Registry for Internet Numbers
APNIC = Asia-Pacific Network Information Centre
LACNIC = Latin America and Caribbean Network Information Centre (LACNIC),
RIPE NCC = Réseaux IP Européens Network Coordination Centre (the RIR for Europe, the Middle East and parts of Central Asia)

Fig. 1. Projected RIR Unallocated Address Pool Exhaustion (as of *May 25, 2012*)

Thus, a key desirable capability is the increase in address space such that it is able to cover all elements of the universe set under consideration. For example, all computing devices could have a public IP address so that they can be uniquely tracked[1]; today inventory management of dispersed IT assets cannot be achieved with IP mechanisms alone. With IPv6 one can use the network to verify that such equipment is deployed in place and active; even non-IT equipment in the field can be tracked by having an IP address permanently assigned to it. IPv6 creates a new IP

[1] Note that this has some potential negative security issues as attackers could be able to own a machine and then exactly know how to go back to that same machine again. Therefore, reliable security mechanisms need to be put in place in IPv6 environments.

address format, such that the number of IP addresses will not exhaust for several decades or longer, even though an entire new crop of devices are expected to connect to Internet over the coming years. IPv6 also adds improvements in areas such as routing and network configuration. IPv6 has extensive automatic configuration (auto-configuration) mechanisms & reduces the IT burden making configuration essentially plug-and-play". Specifically, new devices that connect to intranet or Internet will be "plug-and-play" devices. With IPv6 one is not required to configure dynamic non-published local IP addresses, the gateway address, the sub-network mask or any other parameters. The equipment automatically obtains all requisite configuration data when it connects to the network. Auto-configuration implies that a Dynamic Host Configuration Protocol (DHCP) server is not needed and/or does not have to be configured. IPv6 was originally defined in [7] and [8]. A large body of additional Requests for Comments (RFCs) has emerged in recent years to add capabilities and refine the concept.

2 Expansion of IP Video-Based Solutions and Facilities

In the present days, a variety of video-based solutions expand in a wider market scale, as enterprises (and/or organizations or other entities) attempt to increase productivity, decrease travel cost and expand video applications in more "unified communications" platforms. As the related markets continue to develop and -*gradually*-, to mature, the "frontier" between unified communications and tele-presence applications become "unclear". For both previous market-led application sectors, the corresponding video devices & equipment employ many of the same protocols and codecs, thus offering adequate integration and the ability to use infrastructure devices originating from each solution. Video services actually offered, include several conferencing applications as well as streaming and recording ones. Conferencing devices permit three or more video devices to participate in a meeting, simultaneously; some among them are also able to provide management of conferencing resources, thus allowing for a more efficient use. Streaming & recording devices offer the capability to record, replay, and stream important meetings, messages, or (related) updates. Video components consist of devices such as video endpoints[2], call control, conferencing, gateways, and management platforms. Tele-presence and video in general, initiate a lot of new terminology & concepts that are quite innovative, as there are no similar options from previous uses or technologies. This also implicates that numerous new facilities, services, products & attributes are now introduced with the development of video endpoints, conferencing devices and error concealment.

A suitably designed network is an essential prerequisite of any proper video design. The use of existing network protocols, tools and features can make simpler the related video deployments and can offer guarantee for a successful growth. As (interactive) video devices are sensitive to delay, loss and jitter, it is essential to

[2] An endpoint consists of a screen, microphone, speakers, and one or more video and audio processing devices called as codecs. These components are usually combined into a single unit that can range from a phone with a screen (at the basic end), to a large TV-like device, to an immersive multi-screen system with integrated tables and seating.

"preserve" all these undesired effects to a minimum level. Identifying video traffic on the network and ensuring end-to-end QoS, can give a proper video experience. Allowing admission to the network only when bandwidth is available and enough to guarantee media flows that meet Service Level Agreements (SLAs) are critical factors to any successful video deployment. There are a number of possible scenarios available for (interactive) video deployments, based on a number of factors such as the number and type of endpoints, while focusing on all -or on most- aspects of call control, video services and network design. In particular, business-to-business (b2b) video communications is now becoming more important as video continues to be deployed and used by more companies for pure market support conditions. There are a number of ways to allow b2b video communications, depending on the call control platforms and endpoints used in an enterprise. The list of technologies to be used in IP video solutions is long. Protocols provide a complete set of specifications and suite of standards for communications between devices. The primary call control protocols used in most IP video solutions today are H.323, Session Initiation Protocol (SIP), and Skinny Client Control Protocol (SCCP). Selecting the right protocol for the design of the IP video solution is crucial for success. A wrong protocol choice could result in scalability issues and/or the inability of users to execute expected features.

H.323 [9] is not a single standard or protocol but rather a suite of protocols and recommendations established by the International Telecommunication Union (ITU) Telecommunication Standardization Sector (ITU-T). It is very strict in the definition of its features, expected behavior and implementation, which puts H.323 in an advantageous position for interoperation between telecommunication vendors and providers. Because H.323 implementation is so well defined, it leaves very little room for misinterpretation of what is expected from the vendors when they interoperate. H.323 uses a peer-to-peer protocol model that supports user-to-user communication without a centralized call control element. Session Initiation Protocol (SIP) is a peer-to-peer protocol [10]. In its simplest implementation, SIP endpoints do not need a call control entity to contact each other, assuming they know their location. However, SIP also defines a client/server relationship so that the endpoints can make use of services, resources, and dialable destinations that are unknown to the endpoints. SIP is defined by the Internet Engineering Task Force (IETF) and is conglomeration of RFCs. Skinny Client Control Protocol (SCCP) was first developed by Cisco for IP Telephony applications [11]. As IP Telephony matured, it integrated video as well. SCCP defines Transmission Control Protocol (TCP) as the transport protocol and a call agent in an architectural relationship with the endpoints (also known as a master/slave relationship). The call agent is the most fundamental difference between SCCP and the rest of the call control protocols discussed in this section. Because SCCP employs a central call agent, it inherently enables very advanced call functions for video endpoints that might not be available in other call control protocols.

3 IPv6 Advantages for Enhanced Video Communications

Today's IPv6 deployment drivers focus on performance approaching that of IPv4 albeit on an expanded scale, operational cost savings through simpler network models when deploying applications, and on enabling new product and service innovation.

With the upcoming exhaustion of IPv4 addresses, IPv6 is actually making real business sense, and many companies are now in the process of transitioning to it. In particular, IPv6 offers many advantages for video communications or collaboration applications, including support for a much larger address space, more advanced security, improved interoperability and enhanced QoS to name few. IPv6 with its 128-bit addressing system combines security/authentication, QoS (reserving bandwidth), plug-and-play for network device configuration, a hierarchically structured routing system, and is thereby ideal for use in IP-enabled videoconferencing. The risks of ignoring IPv6 and not planning ahead could range from inability to connect new devices to diminished business-to-business capabilities. A proper approach for growth when deploying a new IP video solution, could implicate a good knowledge of the network to be used together with the assurance that the selected manufacturers and products have a clear roadmap for IPv6. The various IPv6 advantages can be summarized as below:

- **Scalability and expanded addressing capabilities:** IPv6 has 128 bit addresses versus 32 bit IPv4 addresses. With IPv4 the theoretical number of available IP addresses is 2^{32} ~10^{10}. IPv6 offers a 2^{128} space. Hence, the number of available unique node addressees is 2^{128}~10^{39}. IPv6 has more than 340 undecillion (340,282,366,920,938,463,463,374,607,431,768,211,456) addresses, grouped into blocks of 18 quintillion addresses. Thus, it simplifies aspects of address assignment (stateless address auto-configuration), network renumbering and router announcements when changing network connectivity providers. The IPv6 subnet size has been standardized by fixing the size of the host identifier portion of an address to 64 bits to facilitate an automatic mechanism for forming the host identifier from link-layer media addressing information (MAC Address).
- **"Plug-and-play":** IPv6 includes a "plug-and-play" mechanism that facilitates the connection of equipment to the network. The requisite configuration is automatic; it is a server-less mechanism.
- **IPv6 makes it easy for nodes to have multiple IPv6 addresses on the same network interface.** This can create the opportunity for users to establish overlay or Communities of Interest (COI) networks on top of other physical IPv6 networks. Department, groups or other users and resources can belong to one or more COIs, where each can have its own specific security policy.
- **Security:** Network security is also integrated into the design of the IPv6 architecture, including the option of IPSec [12]. IPv6 includes security in its specifications such as: payload encryption and authentication of the source of the communication; end-to-end security, with built-in, strong IP-layer encryption and authentication (embedded security support with mandatory IPsec implementation). It follows that IPv6 network architectures can easily adapt to an end-to-end security model where the end hosts have the responsibility of providing the security services necessary to protect any data traffic between them; this results in greater flexibility for creating policy-based trust domains that are based on varying parameters including node address and application.

- **In IPv6, creating a VPN is easier and more standard than in IPv4**, because of the (Authentication Header (AH) and Encapsulating Security Protocol (ESP)) Extension Headers. The performance penalty is lower for the VPN implemented in IPv6 compared to those built in IPv4.
- **Optimized protocol:** IPv6 embodies IPv4 best practices but removes unused or obsolete IPv4 characteristics. This results in a better-optimized protocol. Also, merging two IPv4 networks with overlapping addresses (say, if two organizations merge) is complex; it will be much easier to merge networks with IPv6.
- **Real time applications:** To provide better support for real time traffic (e.g., VoIP, IPTV), IPv6 includes "labeled flows" in its specifications. By means of this mechanism, routers can recognize the end-to-end flow to which transmitted packets belong. This is similar to the service offered by Multi-Protocol Label Switching (MPLS) [13], but it is intrinsic with the IP mechanism rather than an add-on. Also, it preceded this MPLS feature by a number of years.
- **Mobility:** IPv6 includes more efficient and robust mobility mechanisms (enhanced support for Mobile IP and Mobile Computing Devices). Several features of IPv6, including its support for near unlimited numbers of potentially connected devices at any given time, combined with mobility, make the standard a logical candidate for some of these new uses, mainly in video-oriented communications. Mobile IPv6 as defined in [14] is now starting to be deployed. Work performed in [14] notes that without specific support for mobility in IPv6, packets destined to a mobile node would not be able to reach it while the mobile node is away from its home link. In order to continue communication in spite of its movement, a mobile node could change its IP address each time it moves to a new link, but the mobile node would then not be able to maintain transport and higher-layer connections when it changes location. Mobility support in IPv6 is particularly important, as mobile computers are likely to account for a majority or at least a substantial fraction of the population of the Internet during the lifetime of IPv6. The Mobile IPv6 protocol defined in RFC 3775 ([14]) allows nodes to remain reachable while moving around in the IPv6 Internet. Each mobile node is always identified by its home address, regardless of its current point of attachment to the Internet. While situated away from its home, a mobile node is also associated with a care-of address, which provides information about the mobile node's current location. IPv6 packets addressed to a mobile node's home address are transparently routed to its care-of address. The protocol enables IPv6 nodes to cache the binding of a mobile node's home address with its care-of address, and to then send any packets destined for the mobile node directly to it at this address. To support this operation, Mobile IPv6 defines a new IPv6 protocol and a new destination option. All IPv6 nodes, whether mobile or stationary, can communicate with mobile nodes.
- **Streamlined header format and flow identification with Extensibility:** IPv6 has been designed to be extensible and offers support for new options and extensions, thus allowing for more potential features and capabilities.

ISPs and carriers have been preparing for IP-address exhaustion for a number of years and there are transition plans in place. The expectation is that IPv6 can make IP devices less expensive, more powerful, and even consume less power; the power issue is not only important for environmental reasons but also improves operability (e.g., longer battery life in portable devices, such as mobile phones).

4 Quality of Service and IP Multicasting in IPv6 Environments

Tomorrow's Internet[3] will carry real-time traffic such as voice and video in addition to the multiple uses it serves today. IPv6 addresses the technical issues necessary to allow enough bandwidth for different applications-services, including voice/video. This capability, called as "QoS", allows IPv6 routers to recognize certain types of traffic and give each type a specific amount of the available bandwidth. In this scope, real-time traffic will command a higher priority than all other traffic. This addresses the QoS issue for voice-video, ensuring that such services are relegated to highest-bandwidth networks in a manner that is not actually possible with IPv4. Obviously, streaming audio and video requires low latency & high throughput. QoS [15] is strongly supported in IPv6. The IPv6 header has two QoS-related fields, as below, where each type of traffic can have a different QoS value; the network, then, provides preference when it identifies packets that have a higher QoS value. We distinguish:

- The **20-bit Flow label**, usable in IntServ-based environments [16]. In such environments performance's guarantee to traffic and resource reservations are provided on per-flow basis. A guaranteed and controlled load service capability is so supported. IntServ approaches have scalability issues.
- The **8-bit Traffic Class indicator**, usable in DiffServ-based environments. DiffServ environments [17], [18] are more common. The traffic class field may be used to set specific precedence or Differentiated Services Code Point (DSCP) values. These values are used in the exact same way as in IPv4. Performance guarantees are provided to traffic aggregates rather than to flows. DiffServ classifies all the network traffic into classes. Two distinct types (per hop behaviors) are supported, that is: (i) *Expedited Forwarding (EF)* - It aims at providing QoS for the class by minimizing jitter and is generally focused on providing stricter guarantees, and; (ii) *Assured Forwarding (AF)* - It inserts at most 4 classes with at most 3 levels of packets dropping categories.

There are no signaling protocol for resource allocation (admission control[4]) and QoS mechanisms control. The following priority levels are typical, but variances are also possible:

---

[3] See, for example: `http://ipv6.com/articles/general/IPv6-The-Future-of-the-Internet.htm`

[4] To ensure that the voice and video traffic does not use all the bandwidth in the link and cause other important data such as business applications to experience dropped packets, organizations can use calls admission control. Call admission control limits the number of calls allowed through a particular link between sites.

- Level 0 - No specify priority
- Level 1 - Background traffic (news)
- Level 2 - Unattended data transfer (email)
- Level 3 - Reserved
- Level 4 - Attended bulk transfer (FTP)
- Level 5 – Reserved
- Level 6 - Interactive traffic (Telnet, Windowing)
- Level 7 - Control traffic (routing, network management)

However, no deployment has been using the flow label so far and this is an area of more research.

The multicast environment consists of transmitters (senders) and receivers. Just as was the case in the IPv4 case, an IPv6 multicast group is a group of receivers that wish to receive a specific data stream that is transmitted using IPv6 packets at the network layer [19]. This group has no physical or geographical specificity: receivers can be located anywhere on the underlying (public or private) network. IPv6-based devices that wish to receive specific traffic are known as group members and packets delivered to group members are identified by a single multicast group address. The network can deliver information to a large (unlimited) number of receivers, by transmitting only one copy of the multicast information on each subnet. Multicast packets are delivered to a group using best-effort methods, just as is the case for IPv6 unicast packets. Receivers that wish to receive data intended for a particular group must join this group by signaling their local router. This is achieved with the MLD protocol [20]. Routers utilize MLD protocol to learn whether members of a group are present on their directly-attached subnets. Devices join multicast groups by sending MLD report messages. Membership in a multicast group is dynamic: devices can join & leave at will. A device can be a member of more than one multicast group at a time. Properly-configured/authorized IPv6 hosts, regardless of whether they are a member of a group, can send to a group; however, only group members receive the message. A multicast address is assigned for the receivers in a group. Senders utilize it as the destination address of a packet intended to reach all group members.

5 Summary

New technologies, new viewing paradigms, and new content distribution approaches are about to take the TV/video services industry by storm. Five emerging trends related to the next-generation delivery of entertainment-quality video are observable, which can be capitalized upon by progressive service providers, telcos, cable operators, and ISPs. These trends are: (i) the worldwide deployment of IPv6; (ii) the (gradual) deployment of streaming and IPTV services; (iii) the gradual migration of consumer viewing habits from watching linear (real-time) programming to non-linear (on-demand/stored/time-shifted) programming (whether from a local or networked digital video recorder); (iv) the greater interest and reliance on web-produced video content; and; (v) the plethora of screens upon which video can be consumed: e.g. TV, personal computer, tablet, game consoles or cell/smart-phone screen. Among these, IPv6 seems to be a critical factor for further growth and success, especially in the context of the development-penetration of video-to-video communications that are now gaining ground in the market place for various categories of users/consumers, including both corporate and residential ones. Indeed, in the developed world, at the consumer end not only the viewer now has a variety of output devices to display

video content, but also the viewing habits are changing. IPv6 can provide a multiplicity of benefits and facilities, together with enhanced QoS that can "make the difference" for further growth in the ICT sector. In addition, challenge becomes greater as mobile video viewing is also growing at a rate of over 50 per cent a year in recent years. A transition from broadcast to multicast, and even to low-density narrowcast *-these last two either in linear or time shifted/on-demand-* is occurring. Over the next few years these changes are expected to have tidal impacts on the infrastructure used to deliver content, from broadcast TV, to IP-based networks operation over fiber, to satellite delivery, to 3G/4G wireless network, to server-based on-demand content distribution systems.

References

1. Postel, J.: RFC 791 – Internet protocol, DARPA Internet Program Protocol Specification. Internet Engineering Task Force (IETF) (1981)
2. http://www.ipv6forum.org/
3. Huston, G.: Addressing as a Fundamental part of the Internet. NSF/OECD (2007)
4. Gunderson, S.H.: Global IPv6 Statistics - Measuring the current state of IPv6 for ordinary users. RIPE 57, Dubai (2010)
5. Organization for Economic Cooperation and Development (OECD): Internet Address Space-Economic Considerations in the Management of IPv4 and in the Deployment of IPv6. Ministerial Background Report (DSTI/ICCP(2007)20/Final/). OECD, Paris (2008)
6. Asadullah, S., Ahmed, A., Popoviciu, C., Savola, P., Palet, J.: RFC 4779 - ISP IPv6 Deployment Scenarios in Broadband Access Networks. IETF (2007)
7. Deering, S., Hinden, R.: RFC1883 - Internet Protocol, Version 6 (IPv6) Specification. IETF (1995)
8. Deering, S., Hinden, R.: RFC 2460 - Internet Protocol, Version 6 (IPv6) Specification. IETF (1998)
9. ITU-T: Recommendation H.323-Packet-based multimedia communications systems (2009)
10. Johnston, A.: SIP - Understanding the Session Initiation protocol, 2nd edn. Artech House (2004)
11. http://www.cisco.com/en/US/tech/tk652/tk701/tk589/tsd_technology_support_sub-protocol_home.html
12. Kent, S., Seo, K.: RFC 4301 – Security Architecture of the Internet Protocol. IETF (2005)
13. Alwayn, V.: Advanced MPLS Design and Implementation. Cisco Press (2004)
14. Johnson, D., Arkko, J.: RFC 3775 – Mobility Support in IPv6. IETF (2004)
15. Szigeti, T., Hattingh, C.: End-to-End QoS Network Design – Quality of Service in LANs, WANs and VPNs. Cisco Press, Indianapolis (2004)
16. Braden, R., Clark, D., Shenker, S.: RFC 1633 – Integrated Services in the Internet Architectures: An Overview. IETF (1994)
17. Nichols, K., Blake, S., Baker, F., Black, D.: RFC 2474 – Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers. IETF (1998)
18. Blake, S., Black, D., Carlson, M., Davies, E., Wang, Z., Weiss, W.: RFC 2475 - An Architecture for Differentiated Service. IETF (1998)
19. Hinden, R., Deering, S.: RFC 4291 – IP Version 6 Addressing Architecture. IETF (2006)
20. Deering, S., et al.: RFC 2460 – Multicast Listener Discovery (MLD) for IPv6. IETF (1999)