Patents on IPv6-Related Technologies

Michele Amoretti[1], Gianluigi Ferrari[2], Jean-Luc Richier[3], Andrzej Duda[3]
1: Interdept. Centre SITEIA.PARMA, University of Parma, Italy
2: Dept. of Information Engineering, University of Parma, Italy
3: Grenoble Institute of Technology,
CNRS Grenoble Informatics Laboratory UMR 5217, France

September 27, 2013

Abstract

IPv6 is an Internet Layer protocol for packet-switched networks providing end-to-end datagram transmission across multiple domains. IPv6 was formally described for the first time in the Request for Comments (RFC) 2460, published in December 1998. In addition to offering a larger addressing space, IPv6 also defines some features not present in the previous version of the protocol (IPv4). For example, IPv6 simplifies the aspects of address assignment, network renumbering, and router announcements when changing network connectivity providers. Moreover, it simplifies packet processing in routers by placing the need for packet fragmentation at end points. IPv6-related patents cover issues or extensions not defined by RFCs. In this research article, we present and discuss the state of the art of such patents.

Keywords: IPv6, Addressing, Routing, Transition, Mobility, Sensor Networks

1 Introduction

The Internet Protocol (IP) suite specifies a set of protocols used to transport datagrams (packets) from the originating host across network boundaries, if necessary, to the destination host specified by a network address. The IPv6 [1] Internet Layer protocol for packet-switched networks has been developed to deal with the long-anticipated problem of IPv4 address exhaustion. Indeed, IPv6 uses 128-bit addresses — in contrast to IPv4's 32-bit addresses — thus supporting a theoretical maximum of 2^{128} networked devices. Moreover, IPv6 simplifies the aspects of address assignment, network renumbering, router announcements when changing network connectivity providers, and packet processing in routers by placing the need for packet fragmentation at end points. For these reasons, the deployment of IPv6 networks is growing worldwide.

Protocols are specified within the Internet Engineering Task Force (IETF) in documents called Request for Comments (RFC). RFCs contains three sub-series: i) Standard track, leading to standard RFCs (STD), the highest maturity level ii) For Your Information (FYI), informational RFCs, iii) Best Current Practice (BCP), collects administrative documents and other texts considered as official rules.

The Internet Engineering Steering Group (IESG) supervises the IETF activities and the Internet standards process according to the rules and procedures ratified by the Internet Society (ISOC) trustees. The Internet community uses the standardization process described in BCP 9 (RFC 2026 and updates) [2].

The Internet Assigned Numbers Authority (IANA) defines other information such as addresses, numbers, names required for the operation of the Internet.

BCP 79 (RFC 3979 and 4879 [3, 4]) states the policy with respect to Intellectual Property Rights (IPR):

> In general, IETF working groups prefer technologies with no known IPR claims or, for technologies with claims against them, an offer of royalty-free licensing. But IETF working groups have the discretion to adopt technology with a commitment of fair and non-discriminatory terms, or even with no licensing commitment, if they feel that this technology is superior enough to alternatives with fewer IPR claims or free licensing to outweigh the potential cost of the licenses.
>
> Over the last few years the IETF has adopted stricter requirements for some security technologies. It has become common to have a mandatory-to-implement security technology in IETF technology specifications. This is to ensure that there will be at least one common security technology present in all implementations of such a specification that can be used in all cases. This does not limit the specification from including other security technologies, the use of which could be negotiated between implementations. An IETF consensus has developed that no mandatory-to-implement security technology can be specified in an IETF specification unless it has no known IPR claims against it or a royalty-free license is available to implementers of the specification unless there is a very good reason to do so. This limitation does not extend to other security technologies in the same specification if they are not listed

as mandatory-to-implement.

For these reasons, patents mainly cover issues or extensions not defined by RFCs.

2 IPv6-related patents

In the following sub-sections, we illustrate and comment some IPv6-related patents, concerning both general aspects and more specific topics — ranging from core networks to mobile networks, also considering performance and security aspects.

2.1 General aspects

RFC 2460 [1], which specifies the IPv6 address, does not consider the specific manner for a user terminal to acquire an IPv6 address. There is a general agreement that address allocation is a free process. Each RFC can only describe one possible solution. However, all should respect the *IP Version 6 Addressing Architecture* (RFC 4291, updated by: RFC 5952, RFC 6052 [5, 6]). There are different agreed solutions:

- manual configuration;
- stateless address auto-configuration, with different flavors: MAC based, crypto-secure, anonymous, etc.;
- DHCP configuration;
- PPP for point to point.

Patent US 7958220 B2, titled *Apparatus, method and system for acquiring IPv6 address* [7], is a system and a mechanism for acquiring an IPv6 address. There, IPv6 addresses are allocated to user terminals uniformly by a Broadband Remote Access Server (BRAS) or a network server, improving the security of IPv6 address in use and decreasing the probability of imitational user terminals in the Internet, while ensuring the uniqueness of each IPv6 address. The network server may be a Remote Authentication Dial In User Service (RADIUS) server, a Terminal Access Controller Access Control System (TACACS) server, or a Dynamic Host Configuration Protocol (DHCP) server, and so on. Different embodiments of the system are considered by the patent. The whole architecture is illustrated by the structure diagram in Fig. 1. The user terminal is provided with a request module which sends an IPv6 address allocation request, receives an IPv6 address allocation acknowledgement, and acquires a desired IPv6 address from the acknowledgement. The BRAS determines the IPv6 address according to the IPv6 address allocation request, and returns the determined IPv6 address to the user terminal via the IPv6 address allocation acknowledgement. In another embodiment, the BRAS may just act as a bridge between request modules and the network server, forwarding IPv6 address allocation requests in one direction, and IPv6 address allocation acknowledgements in the other. Also, the user terminal may interact directly with the network server without the BRAS. If the IPv6 prefix set for an interface or ISP domain by an IPv6 address management device changes, the IPv6 address management device may periodically send IPv6 address allocation acknowledgements — carrying changed attribute information of the IPv6 prefix — to all user terminals belonging to the interface or ISP domain.

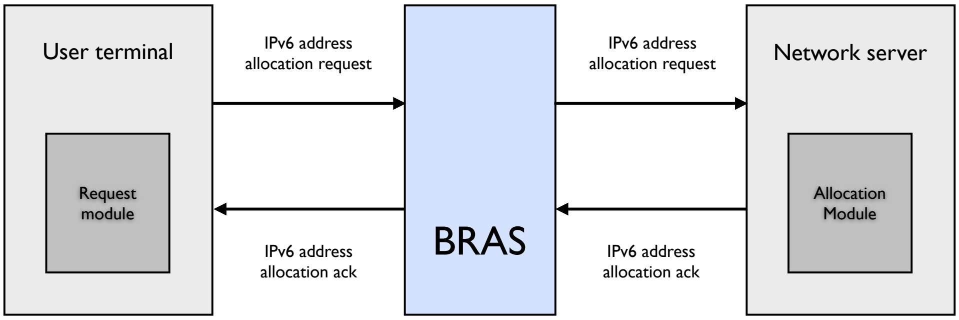
User terminal
Request module
IPv6 address allocation request
IPv6 address allocation ack
BRAS
IPv6 address allocation request
IPv6 address allocation ack
Network server
Allocation Module

Figure 1: Structure diagram of the system patented US 7958220 B2 [7].

Despite the advantages of IPv6 and its likely future dominance on the Internet, its deployment has been relatively slow. As such, IPv6 accounts for a very small portion of the used addresses and traffic on the Internet, which is still dominated by IPv4. This is due at least in part to costs associated with deploying IPv6. Organizations which continue to use established IPv4 infrastructures, as well as organizations that invest fully in IPv6 have to compatibly operate with both IPv4 and IPv6 addresses. Patent US 8351430, named *Routing using global address pairs* [8], presents a routing strategy based on IPv6-to-IPv4 and IPv4-to-IPv6 address mapping. When a network packet is produced by a sending application, the sending side address processing module accesses an address mapping from a sending side local store, to map the IPv6 address of the destination to a couple of IPv4 address (the site public IP address and a node private IP address). The address processing module performs such a mapping with the help of a name server which contains a number of entries binding domain names to IP addresses, including globally unique IPv6 address. The receiving site, if necessary, performs the inverse mapping (from IPv4 to IPv6). In between sites, routers are supposed to be IPv4-based. The whole architecture is illustrated by the structure diagram in Fig. 2.

A very related patent is US 7764686 B1 *Migration to IPv6 using combination of globally significant and locally significant IPv4 addresses* [9]. In one implementation, certain IPv4 nodes are enhanced by use of a dual address including a globally significant site address and a locally significant address used only within a particular site. This dual

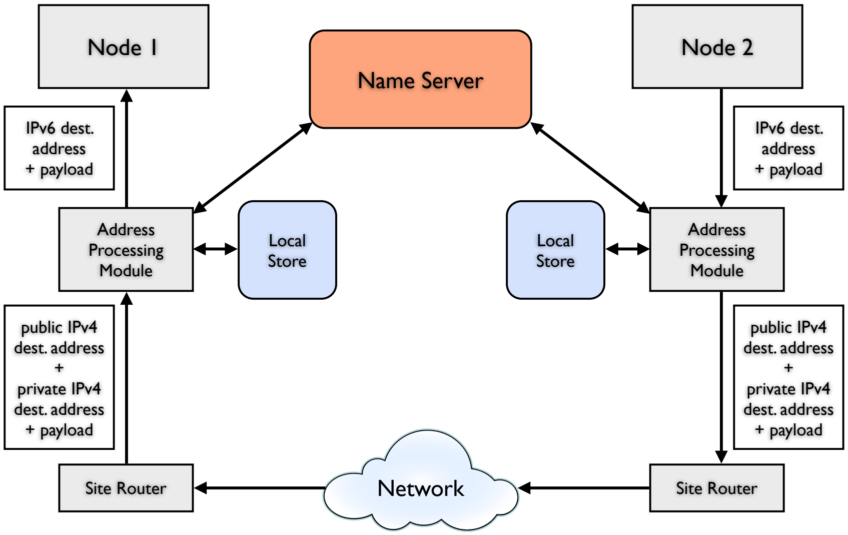
Node 1
Name Server
Node 2
IPv6 dest. address + payload
IPv6 dest. address + payload
Address Processing Module
Local Store
Local Store
Address Processing Module
public IPv4 dest. address + private IPv4 dest. address + payload
public IPv4 dest. address + private IPv4 dest. address + payload
Site Router
Network
Site Router

Figure 2: Structure diagram of the system patented US 8351430 [8].

IPv4 address may be readily mapped to or from an IPv6 address. The address mapping scheme may be used to automatically tunnel IPv6 packets through IPv4 infrastructure and to use enhanced IPv4 nodes to contact IPv6 infrastructure.

The coexistence of IPv4 and IPv6 addresses is supported also by the *Locator/Identifier Separation Protocol (LISP)* [10], developed by the Internet Engineering Task Force LISP Working Group.[1] LISP is an address-family-agnostic routing architecture that implements a new semantics for addressing, by creating two namespaces: Endpoint Identifiers (EIDs), which are the current addresses assigned to end-hosts today, and Routing Locators (RLOCs), which are the addresses assigned to devices (mainly routers) that make up the global routing system. Splitting EID and RLOC functions yields many benefits, such as improved routing scalability, improved multihoming efficiency, and IP mobility. IPv6 transition is very naturally enabled by LISP, which allows to use the same or different address families for the EIDs and the RLOCs. One way to gain basic IPv6 experience while limiting capital expenses (CapEx) and operational expenses (OpEx), and minimizing changes to the existing infrastructures, is to create IPv6 islands within the corporate network and connect them using LISP over the existing IPv4 core.

2.2 Access networks

With IPv6 stateless auto-configuration it is possible to realize Plug & Play, but also to make the network more flexible. However, to apply it into access networks — rather than

[1] `https://datatracker.ietf.org/wg/lisp/charter/`

to friendly network environments, for which it has been designed — it is necessary to introduce some control mechanisms, in order to prevent security problems. In general, IPv6 stateless auto-configuration works in the following way. A router (or a layer 3 access node) sends two types of Router Advertisement (RA) messages to a directly attached link: (1) periodic unsolicited Router Advertisement messages, and (2) Router Advertisement messages in response to Router Solicitations (RS). The RS/RA messages are encapsulated in ICMPv6 packets. The RA messages carry global IP prefixes. Thus, all the terminal interfaces on the link can obtain the IPv6 prefixes and form their global IPv6 addresses, by appending their own interface identifier to the IPv6 prefixes.

Patent EP 1648134 B1 *Network service selection and authentication and stateless auto-configuration in an IPv6 access network* [11] proposes a solution to the control problem described above. In particular, the invention provides a method for Network Service Provider (NSP) service selection and authentication in an IPv6 access network. As illustrated in Figure 3, terminals in a subscriber network send RS messages to an access node. The RS messages includes a Network Service Selection and Authentication (NSSA) Information option, which contains user information for the network service selection and authentication. The access node extracts such user information from the NSSA Information option, and communicates with a corresponding AAA server for authentication. Upon authentication, a NSP prefix is obtained, and the access node sends out the obtained NSP information and prefix information to the subscriber network, encapsulated in RA messages. The NSP Information option contains the address of NSP edge router and the NSP name.

Patent EP 1641192 B1 *Method and device for detecting connectivity termination within an internet protocol version 6 access networks* [12] is a method to detect connectivity termination in IPv6 access networks. A good connectivity termination detection mechanism should be able to detect the abnormal logoffs of the subscriber — for example, the abnormal logoffs due to sudden power off or hardware failure. The mechanism shall avoid that if subscriber A does an abnormal logoff and this event is not detected, subscriber B may steal the service with the IP address of subscriber A. The IPv6 access network includes an access node and at least one subscriber terminal. In accordance with RFC 2461 *Neighbor Discovery for IP Version 6 (IPv6)* [13], a neighbor cache list is stored in the access node. Moreover, a subscriber connectivity cache list is stored in the access node. All the entries of the neighbor cache list are used to indicate whether the subscriber terminals connected to the access node are reachable, wherein each entry includes an “IPv6 address” field to identify the subscriber terminal to which this entry corresponds, and a “Neighbor_State” field to identify whether the subscriber terminal is reachable. The access node periodically checks if all the subscribers have a related entry in the neighbor cache list. If an entry does not exist, it means that the subscriber logged off abnormally. Otherwise, the subscriber entry is checked for being in the REACHABLE state. If not, other checks are performed, in order to update the subscriber connectivity state from ACTIVE to either PROBE or DELAY, which trigger later checks, respectively after 3 and 8 seconds.

Along with the opportunities provided by IPv6, challenges come as well. The introduction of IPv6 is intrusive. Most current accounting and management systems do not directly support the new protocol and new service needs. Additionally, the net-

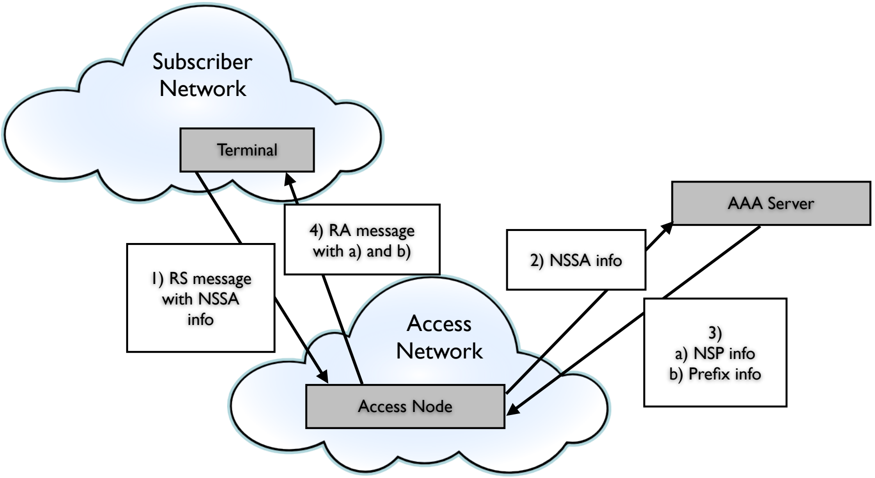
Subscriber Network
Terminal
Access Network
Access Node
AAA Server
1) RS message with NSSA info
2) NSSA info
3) a) NSP info b) Prefix info
4) RA message with a) and b)

Figure 3: Solution patented EP 1648134 B1, for NSP service selection and authentication in an IPv6 access network [11].

work infrastructure does not adequately handle the requirements of running the IPv4 and IPv6 protocols simultaneously. For example, services such as VoIP have been very successful for cable providers, and it is important that their performance and operation is not affected by the coexistence of the two IP versions. A stable migration path to ensure the successful introduction of this extensible feature rich protocol is paramount. In this context, patent US 7941512 *Use of IPv6 in access networks* [14] defines a method for detecting a connection to a cable modem termination system (CMTS), determining whether the CMTS is IPv6-capable; booting up in either IPv6 only mode or IPv6 with IPv4 fallback mode, if the CMTS is IPv6-capable; booting up in IPv4 mode, if the CMTS is not IPv6-capable. Moreover, the patent defines a method to establish a link layer connection to an access server, obtaining a management address (at least one of an IPv6 and an IPv4 address), obtaining a TFTP server address (either IPv6 or IPv4), downloading a configuration file from the TFTP server, registering with the access server as IPv6 capable, maintaining an IP address/prefix-MAC mapping database, and finally determining whether the IPv6 address belongs to a particular media access control (MAC) address based on the IP address/prefix-MAC mapping database.

2.3 Cellular networks

A cellular network, especially from the third generation (3G) on, is typically constituted by a Core Network (CN) and several Radio Access Networks (RANs). The expansion of the use of the Internet Protocol (IP) is pushing the use of “Internet communications” into cellular networks or, more generally, mobile communication systems. The forthcoming use of IPv6 is particularly challenging in the CNs, as several technological issues arise in the evolution of current architectures to support the use of IPv6 and, especially, to take full advantage of its potential.

Patent EP 1744582 B1 *Method and apparatus for performing handover between core network entities in a packet-switched network* [15] focuses on the handover in 3G systems at layer 2 (L2) and layer 3 (L3). In fact, while a RAN takes care of the handover at L2, the CN takes charge of handover at L3. Typical L2 and L3 handover schemes do not support IP address mobility because a User Equipment (UE) moving between CN entities is not identified by its IP address. IPv6 technology allocates and configures IP addresses by the Ethernet-based L3 network control protocol. In this context, L3 handover suffers a long delay and large packet loss. The patent presents a method and an apparatus for performing fast and seamless handover between CN entities in a packet-switched network developed from a 3G mobile communication system. The key idea is that of making RANs and CNs communicate more efficiently in the presence of an handover. In particular, when a UE connected to an old CN through an old RAN moves to a new RAN belonging to a new CN, the old RAN sends a handover required message to the new RAN. The new RAN acquires a new IP address for the UE from the new CN in response to the handover required message and sends a handover command message including the new IP address to the old RAN. The old RAN inserts an address of the new RAN in the handover command message and forwards the handover command message with the address of the new RAN to the UE. The UE performs an inter-RAN handover in response to the handover command message, thereby communicating with the old CN through the new RAN. The UE then performs an inter-CN handover based on the new IP address included in the handover command message, thereby communicating with the new CN through the new RAN.

Patent US 7483439 B2 *VPN services using address translation over an IPv6 network* [16] relates to providing Multicast Virtual Private Network (MVPN) services using IPv4-in-IPv6 address translation over an IPv6 network. Virtual Private Networks (VPNs) serve as network overlays on IP network infrastructures. In this context, it is desirable to provide scalable IPv4 and IPv6 unicast and multicast VPNs over one or more service provider networks, so that IPv4 VPNs run better when IPv6 is deployed in the service provider network. In [16], a method and system for translation of VPN addresses over a provider network are presented. The method is based on the creation of a multipoint tunnel extending between customer edge routers in a VPN network and over the provider network. Moreover, a method for providing VPN communication over an IPv6 networks generally comprises associating a group address with a VPN, creating a multipoint tunnel extending between the VPN and the IPv6 network, and translating VPN source and group addresses into a provider source and group state. IPv4 packets received at a customer edge router of the VPN are encapsulated in an IPv6 packet and sent to the multipoint tunnel for transmission over the IPv6 network.

While the increased address size guaranteed by IPv6, with respect to IPv4, guarantees the co-existence of a huge number of addressed devices, most devices at the local link edge (especially battery-equipped devices with limited processing and communication capabilities, such as “sensor nodes”) lack the resources to support the larger address size. While other methods of addressing for such devices are being investigated, there are no methods that incorporate the ability to route data directly based on an offset bit slice of the IPv6 address. Patent US 7653065 B2 *Method and system for internet protocol address concatenation* [17] provides a method and a system for transmitting packets having a first address length on a CN supporting a second address length, where the second address length is larger than the first address length. In particular, the second address length is derived by determining the length of the first address and extracting an offset to the first address so that a combination of (i) the length of the offset, (ii) the length of a network prefix for the second address and (ii) the length of the first address equals the length of the second address. The method and system of [17] can be implemented as an enhancement to existing network protocol such as IPv4 and IPv6 and the like. The authors consider also the removal of the offset and the network prefix of the second address to derive the first address and transmit a data packet to a destination device based on the first address. The apparatus proposed in [17] aims at transmitting packets having a first address length on a CN supporting a second address length.

In future IPv6-oriented cellular systems it will be more and more important to discover a “desired” network element in a communication system. Patent EP 1759519 B1 *Discovering a network element in a communication system* [18] and patent EP 2425584 B1 *Core network node selection in a mobile communication network* [19] both address the need of discovering specific network elements.

In patent EP 1759519 B1 [18], it is observed that in the transition between the current IPv4-based networks and hosts to such based on IPv6 there are a number of mechanisms and means to be introduced, some of which have already been developed. Therefore, it is unavoidable that both protocols are being used in parallel for some time. Besides Dual Stack (DS) mobile stations, DS routers are needed, which support both IPv4 and IPv6 and are capable of encapsulation and decapsulation of IPv6 packets. Such a DS router can be arranged somewhere in the CN and may not necessarily be “visible” to the RAN and, thus, to a terminal being connected to the RAN. Thus, the host or terminal needs to discover the network address of this DS router in order to use IPv6 via encapsulation over an IPv4 network such as a conventional RAN. Current mobile communication networks, e.g., the cdma2000 packet data network, present a different architecture as compared to standard IP networks. Current solutions involve the use of multicast or configuring of the DS router with an anycast address. Solutions based on Domain Name System (DNS) and Dynamic Host Configuration Protocol (DHCP) are also found to be possible. Since the hosts are connected over an air interface that is operate in the licensed bandwidth spectrum, it is critical that discovery and configuration of such servers is done as optimally as possible (e.g., in terms of bandwidth efficiency). While current solutions do not guarantee this optimality at all, in [18] the investors propose a solution based on the use of an authentication server able to return the network address of the required network element (the “optimal” DS router). A further advantage of the proposed solution is that a terminal is enabled to communicate with an IP Multimedia Subsystem (IMS) based on IPv6 in IPv6 native mode, although the terminal is connected via an access network based on IPv4.

In patent EP 2425584 B1 [19], the problem of efficient selection of an interface node of a CN (of a mobile communication network) for handling data traffic for a mobile device is considered. In particular, when a mobile device is setting up or modifying connections, CN nodes for handling the connections generally need to be selected. For example, in an Evolved Packet System (EPS) network, a Serving Gateway (SGW) and a Packet Data Network (PDN) Gateway (PGW) are selected when the mobile device/user equipment (UE) attaches or establishes a new connection to a PDN. A connection modification may for example be the selection of a new SGW if a mobile device moves to a different SGW service area. Constrains that limit the selection of these network nodes include for example the ability of the SGW to serve the tracking area, in which the mobile device is located, or the ability of the PGW to provide connectivity to the PDN, with which the mobile device requests to communicate. In general, several core network nodes will meet these constrains. The selection of one of these suitable nodes for handling the connection has a substantial impact on the efficiency of data transport to the mobile device. A conventional method for selecting an appropriate core network node uses the so-called "topological proximity" criterion. The mechanism is based on the naming of EPS network nodes according to a naming scheme that represents a tree structure. Two nodes are considered closer to each other if they share a longer common name "root" or "suffix." The basic problem of a topological proximity approach is that the geographic distance of the selected node might be very large, thus hindering the transport efficiency of the information. Current solutions based on naming schemes, such as the Domain Name System (DNS), are unable to handle the actual (complex and not tree-like) topology of an IP network and cannot lead to an efficient selection of an interface CN node. In [19], the interface CN node is selected through the use of a "control node" on the basis of the transport efficiency information, relative to several CN node, stored at the control node. The transport efficiency information is dynamically collected and maintained by the control node by means of a routing protocol.

In future entirely IP-based cellular networks, routing will also play a key role. In patent US 7043247 B2 *Routing header based routing in internet protocol (IP)-cellular networks* [20], a method to provide efficient routing, through the use of routing headers, in fully IPv6 cellular networks is proposed. In IP-applications in 2G/2.5G cellular networks, such as a Global System for Mobile Communications/Generalized Packet Switched Service (GSM/GPRS) network, typically there is a single point of attachment to the external IP networks, such as the Public Internet. An illustrative representation of this scenario is shown in Fig. 4, where the single point of attachment, being a gateway general packet radio service support node (GGSN), is more generally referred to as the gateway router (GR).

The IP-layer in the user equipment (UE) terminates at the GR, i.e., there is a single "IP-level" hop from the UE to the GR. 3G networks (such as a UMTS network) is made up of switching elements which transfer the IP-packets through the use of L2 switching techniques. Some UMTS networks utilize IP-based routing elements, but the IP technology is used purely for transport purposes and is not visible to the UE, meaning that the IP-layer of the UE is still terminated at the GR. In the future, a cellular network will be an interconnected network of IP-routers with the result that the IP-layer of the UE may be terminated by a nearby router. However, since the network is still assumed to have a single point of attachment to external IP-networks, IP packets from the nearest

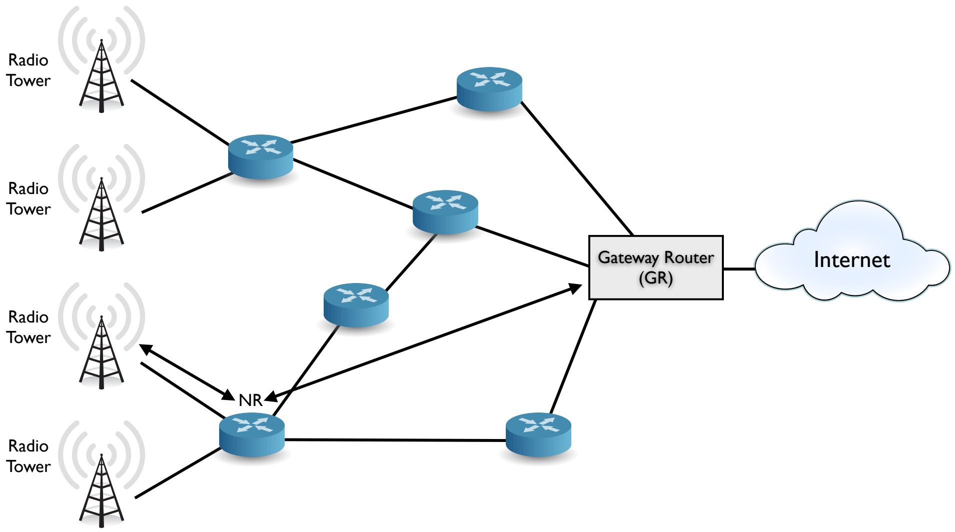

Figure 4: Illustrative representation of a GPS/GPRS scenario for the routing strategy patented in US 7043247 B2 [20].

router must be routed to the GR. This can be achieved by establishing IP-tunnels which involve IP-in-IP encapsulation, but this approach has the disadvantages of requiring the need to set up tunnels and the extra overhead due to encapsulation. In patent US 7043247 B2 [20], this limitation is overcome by using IPv6 throughout the entire cellular network and using routing headers of IPv6 packets to ensure that the packets are routed via the GR to the end destination. This is accomplished by specifying the IP address of the GR as an IP-address of an intermediate router in the routing header. In the same patent, the provision of additional intermediate routers is considered, and their selection is based on criteria such as congestion state and/or capacity and/or monitoring needs.

2.4 Mobile Networks

Mobility Support in IPv6 [21] is a layer 3 mobility protocol which enables Mobile Nodes (MNs) to move between subnets in a transparent manner for higher layers, i.e. without breaking higher layer connections. To this end, a MN uses two IP addresses: a Care-of-Address (CoA) and a Home Address (HoA). The MN's higher layers use the HoA for communication with the Correspondent Node (CN). This address does not change and serves the purpose of identification of the MN. Topologically, it belongs to the Home Network (HN) of the MN. In contrast, the CoA changes on every movement resulting in a subnet change and is used as the locator for the routing infrastructure — topologically, the CoA belongs to the network the MN is currently visiting. One out of a set of Home

Agents (HA) located on the home link maintains a mapping of the MN's CoA to MN's HoA and redirects incoming traffic for the MN to its current location. Fur the purpose of redundancy and load balancing, a set of HAs may be used instead of a single HA.

Mobile IPv6 currently defines two modes of operation: bi-directional tunneling and route optimization. If bi-directional tunneling is used, data packets sent by the CN and addressed to the HoA of the MN are intercepted by the HA in the home network and tunneled to the CoA of the MN. Data packets sent by the MN are reverse tunneled to the HA which decapsulates the packets and sends them to the CN. For this operation, only the HA must be informed about the CoA of the MN. Therefore, the MN sends Binding Update (BU) messages to the HA. However, if the MN is far away from the home network and the CN is close to the MN, the communication path is unnecessarily long, resulting in inefficient routing and high packet delays. The route optimization mode can prevent the described inefficiency by using the direct path between CN and MN. Therefore, the MN sends BU messages to the CN, which then is able to directly tunnel packets to the MN.

Patent EP 1588534 B1 *Provision of mobility for ipv4 traffic in an ipv6 network* [22] is a mechanism for providing mobility for IPv4 traffic using the Mobile IPv6 protocol. At the time the patent was requested, RFC 6275 (Mobile IPv6) was not yet available. However, from the work in progress it was clear that Mobile IPv6 would have provided mobility for IPv6 traffic only, like Mobile IPv4 is for IPv4 traffic only [23]. A first network node maintains the bindings, each one being an association of the IPv4 home address with the IPv6 care-of address of the mobile node. The node which maintains such bindings is called home agent, while the node which assigns CoA is the foreign agent (this nomenclature is widely accepted, as it is the one specified by RFC 2002 [23]). The patent states that when the IPv6 CoA changes, the mobile node sends a binding update packet including the new care-of address and the HoA of the mobile node. A binding is notified by inserting an IPv6 address — with the IPv4 home address embedded in it — in the binding update packet. When such a binding has been created, IPv4 packets can be forwarded by the home agent to the mobile node through an IPv4-in-IPv6 tunnel.

A related patent is EP 1988665 B1 *Method and system for fast handover in hierarchical mobile IPv6* [24], which provides an alternative, more efficient solution to the handover issue, with respect to improved Mobile IPv6 protocols like Hierarchical Mobile IPv6 (HMIPv6) or Fast Mobile IPv6 (FMIPv6). Layer 3 network handover is the process for which a connected cellular call or a data session is transferred from one cell site (base station) to another without disconnecting the session. Mobile IPv6 (shortly described above) has several disadvantages. When the mobile node hands over between access routers (ARs), the handover latency is long and the packet loss rate is high. In an actual application environment, the mobile node needs to hand over between neighboring ARs frequently. In this case, the mobile node has to register with its home agent the mapping relationship between the HoA and CoA frequently, which significantly increases the burden of the HA and is very costly. Meanwhile, duplicate address detection operation is performed on the registered care-of address to verify its validity, which is quite time consuming. The Hierarchical Mobile IPv6 (HMIPv6) scheme introduces Mobility Anchor Point (MAP) to improve handover performance of the MN in the MAP domain. When a mobile node enters a MAP domain, it receives a Router Advertisement (RA) which contains MAP information. The mobile node needs to configure two care-of addresses, namely Regional Care-of Address (RCoA) and On-link Care-of Address (LCoA). The mobile node performs Duplicate Address Detection on the LCoA, and sends a local binding update message to the MAP, when the detection is successful. Upon receiving the local binding update message, the MAP performs Duplicate Address Detection on the RCoA as well, and returns a local binding update acknowledgment message to the mobile node when the detection is successful. Upon receiving the local binding update acknowledgment message, the mobile registers a new RCoA with its home agent. If the mobile node performs a handover within the MAP domain, for example, an AR is changed, then RCoA of the mobile node is kept the same and only LCoA of the MN is reconfigured. The disadvantage of the above scheme lies in that, though it solves to a certain extend the problem of long handover latency for handover within the MAP domain of the Mobile IPv6 scheme, the handover latency is still too long, compared with the requirement of network real time application. In particular, the latency of performing Duplicate Address Detection on the LCoA and RCoA during handover makes up most of the total handover latency. Fast Handovers for Mobile IPv6 is a scheme to improve Mobile IPv6 node fast switching between access points on the network. Before the MN is switched to a new link, it first initiates a handover procedure to acquire the care-of address of the new link beforehand. The handover procedure is realized by exchanging newly-added messages between the new and previous ARs, as well as between the AR and the mobile node. This scheme requires that the mobile node is previously aware of the new link to which it will be moved, and therefore it requires support from Layer 2. The solution proposed by patent EP 1988665 B1 is called Hierarchical-based Fast Handover for Mobile IPv6, as it combines the scheme of HMIPv6 with the scheme of Fast Handover for Mobile IPv6. The drawback of the proposed scheme is that the scheme does not reduce the latency needed to perform Duplicate Address Detection operation on the LCoA and RCoA during handover, and this latency still makes up a great part of the total handover latency. Also, the Hierarchical-based Fast Handover for Mobile IPv6 involves lots of complicated technical steps and is difficult to implement. To improve the situation the patent includes the adoption of an Optimistic Duplicate Address Detection protocol, which is a modification of the existing IPv6 Neighbor Discovery protocol (RFC 2461) [13] and Stateless Address Auto-configuration protocol (RFC 2462) [25]. The patent does not invent a particular version of the Optimistic Duplicate Address Detection protocol. Instead, it does refer to the *Fast Handover for Hierarchical MIPv6* IETF draft [26] and to another patent, namely EP 1473901 B1 [27].

Patent EP 1739901 B1 *Mobile IPv6 optimised reverse tunnelling for multi-homed terminals* [28] provides location privacy and route optimization for packet switching protocols like Mobile IPv6, without requiring the introduction of new or modified infrastructure components in every visited network. The solution shall also work when both communication partners are mobile and shall scale well with respect to deployment, *i.e.*, number of MNs using the solution. It shall also provide the same level of security as standard Mobile IPv6 and be applicable to multi-homed terminals. Optimized Reverse Tunneling (ORT) first requires some initial signaling between MN or MN's HA and CN or CN's HA to negotiate privacy, as well as route optimization requirements of MN and CN. Based on this and additional distance information, candidate scenarios and, subsequently, candidate proxy HAs are determined. After determining the route lengths over the individual candidate proxy HAs, it is decided whether and to which proxy HA(s) tunnels will be switched. Then, binding information is sent and tunnels are switched to the selected target proxy HA(s). Due to mobility, the route lengths are dynamic and the process must be repeated at certain instances in time. The procedures can be realized either in a MN-controlled or an HA-controlled manner. Different scenarios are considered: a) two uni-directional tunneling proxy HAs located in the home networks; b) one bi-directional tunneling proxy HA located in the home network of the MN; c) two unidirectional tunneling proxy HAs located in the visited networks of MN and CN; d) one common bi-directional tunneling proxy HA located in the visited network of the MN; e) one common bi-directional tunneling proxy HA located in a network between the visited networks of MN and CN (Fig. 5).

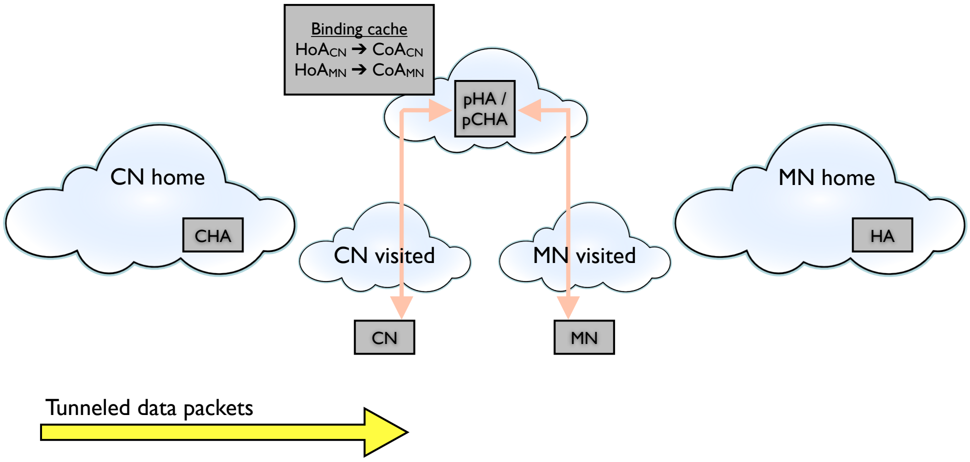

Figure 5: Scenario e) for the system patented EP 1739901 B1 [28].

2.5 Sensor Networks / IoT

Patent US 8036108 titled *"Method and apparatus for providing gateway to transmit IPv6 packet in a wireless local area network system"* [29], is a method for providing a gateway for IPv6 packets between a legacy 6LoWPAN node and a WLAN system. One or more service request messages for data communications are received from 6LoWPAN nodes and a virtual interface is generated for allocating IPv6 addresses to the 6LoWPAN nodes by adding a predetermined IPv6 address prefix to addresses of the 6LoWPAN nodes set in the service request messages. The gateway uses a socket adaptation layer for receiving the IPv6 addresses from the virtual interface and transmitting data packets to 6LoWPAN nodes. It transmits and receives data packets to and from 6LoWPAN nodes.

Patent US 8149816 B2 titled *"Header compression and packet transmission method in sensor network and apparatus therefor"* [30], is a method for efficient packet transmission in a sensor network (cf. Fig. 6). The patent defines a header compression and packet transmission method based on the selection of compression technologies according to characteristics of each node. The method distinguishes a node supporting the adaptation layer function and a node without the adaptation layer function, and determines whether to compress a packet. In this way, the method enables a node transmitting data to transmit the data in a proper form acceptable to a sensor node receiving the data. The method results in a better efficiency of packet transmission.

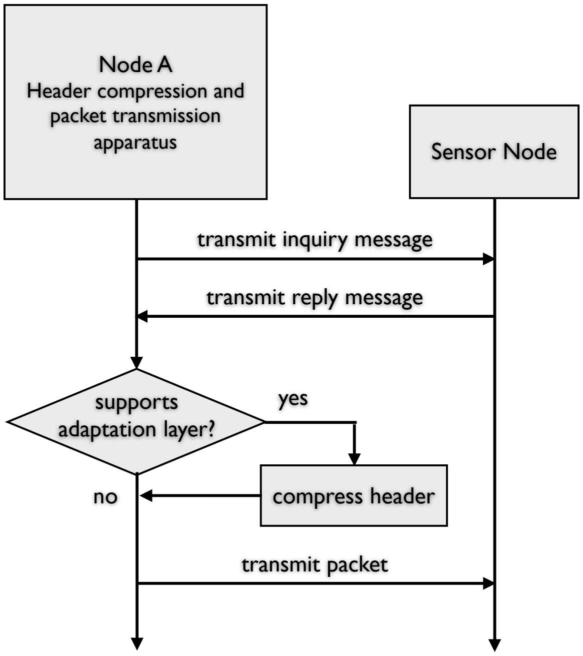

Figure 6: Principle of the system patented in US 8149816 B2 [30].

Patent US 8228954 B2 titled *"Routing operations using sensor data"* [31], is a method for coupling routing with sensor data. The method relies on an Internet Protocol (IP) router receiving sensor data from another IP router or an attached host sensor node. It aggregates sensor data, adds metadata, and stores them in a routing information base. In this way, the IP router can support routing operations based on the sensor information stored in the routing information base.

2.6 Performance and Security

Web sites sometimes make use of a proxy device that initially receives requests on a virtual IP address and distributes them, according to some scheme, among multiple servers. Even after a server has been selected for being associated with a client and a TCP connection has been established to support HTTP messaging, all messages between the client and the server pass through the proxy. When a single proxy device acts as an intermediary for many clients and servers, communications between those clients and servers may be delayed significantly. Furthermore, if the proxy device fails for any reason, then the connection path between the client and the server is severed. To cope with these issues, some approaches attempt to compensate for this vulnerability by providing a “backup” proxy device, to which the “primary” proxy device periodically transmits updated session state information. The transmission of updated session state information between “primary” and “backup” proxy devices also may consume a substantial amount of network bandwidth.

Patent US 8341295 *Server failover using IPV6 mobility features* [32] provides techniques which use the mobility support features of IPv6 to allow a client node and a server node to communicate without the continuing intervention of the load-balancing node (the aforementioned proxy) that selected the server node. A virtual IP address is associated with an entire server ”farm” or ”cluster”. A client node sends an IP packet toward the virtual IP address. Typically, one or more routing nodes lie between the client node and the server cluster. The load-balancing node advertises to the routing nodes that the virtual IP address is reachable through the load-balancing node. As a result, the routing nodes eventually route to the load-balancing node the IP packets that are addressed to the virtual IP address.The load-balancing node intercepts such IP packets. An intercepted IP packet may contain a TCP packet that signals the recipient to engage in a handshake phase with the client node. During the handshake phase, the server node sends an IPv6 packet toward the client node. The IPv6 packet contains an IPv6 Mobility Header, which contains a Binding Update option specifying a Home Address option to indicate the virtual IP address. As a source IP address, the IPv6 packet indicates the Care-of-Address (CoA) of the selected server — which differs from the virtual IP address. When the client node receives the IPv6 packet, the information in the Mobility Header causes the client node to perform IP address replacement operations so that IP packets are addressed to the physical IP address of the selected server node, instead of the virtual IP address. Consequently, the IP packets are routed toward the selected server node, instead of the load-balancing node. Moreover, IP packets that the selected server sends toward the client node contain an IPv6 Mobility Header such as the one described above, which causes the client node to continue to perform IP address replacement operations.

Patent US 8281383 *Secured IPv6 traffic preemption* [33] is related to routers prioritizing transfer of IPv6 packets, where high priority IPv6 packets can preempt lesser-priority IPv6 packets. In detail, the solution (illustrated in Figure 7) defines how to implement, within an access router, a preemptive service for a node requiring absolute priority for transfer of IPv6 packets, regardless of any prior resource reservations for guaranteed quality of service (QoS) of latency-sensitive traffic. The preemptive service identifies priority IPv6 packets by a prescribed flow label field and satisfying a prescribed security condition, enabling the priority IPv6 packets to preempt existing resource reservations for lesser-priority IPv6 traffic that does not qualify for the preemptive service. Hence, preemptive services can be automatically initiated by law enforcement or first responder units in emergency or crisis situations, without the necessity of prior manual configuration of host network nodes or access routers. The solution proposed by this patent is quite different from traditional approaches to QoS provision, which suffer from at least one of the following disadvantages: (1) prior (or manual) complex configuration of routers for static reservation of network resources (*e.g.*, MPLS-TE [34]); (2) dynamic reservation of network resources limited to available network resources that have not already been reserved for another data flow (*e.g.*, RSVP [35,36]); (3) lack of security, which may allow a malicious source to capture reserved resources by spoofing values in an unsecured IP packet (*e.g.*, Differentiated Services [37,38]).

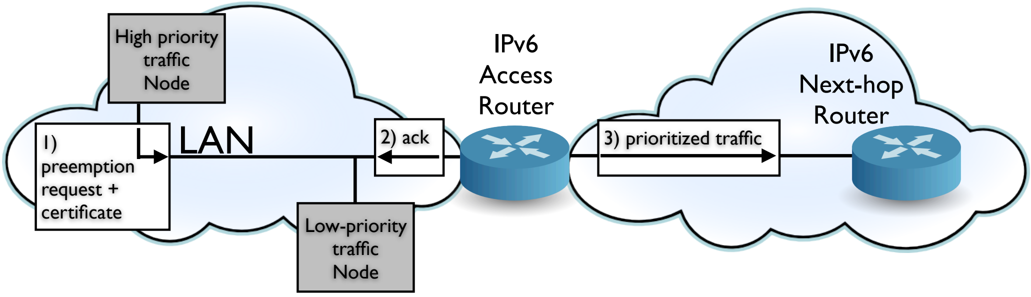
High priority traffic Node
1) preemption request + certificate
LAN
2) ack
Low-priority traffic Node
IPv6 Access Router
3) prioritized traffic
IPv6 Next-hop Router

Figure 7: Example network including an access router providing secured preemptive network services, according to patent US 8281383 [33].

2.7 Comparative Overview

On the basis of the patents' described in the previous sections, it is possible to derive a comparative overview on the main aspects considered across the patents. In Table 1, each class of papers described in the previous sections is characterized in terms of: (i) key objectives; (ii) main protocol layers of interest; and (iii) applicability time horizon.

Table 1: Comparative overview of IPv6-related patents

Patents' Topics	**Key Objectives**	**Network Layers**	**Applicability Time Horizon**
General aspects	addressing	L3	Now
Access networks	connectivity, service discovery	L4 and higher	Next 5 years
Cellular networks	addressing, network element discovery	L3 and higher	Next 5 years
Mobile Networks	mobility, handover	L3 and higher	Next 5 years
Sensor Networks / IoT	gateway, header compression, sensors	L2 and L3	Next 5 years
Performance and Security	load balancing, preemption	L4 and higher	Next 5 years

3 Current and Future Developments

In this section, we discuss some areas related to IPv6 in which there are many ongoing research activities or there is a need for additional functionalities or adaptation. We see them as possible domains of future patents.

Transition to IPv6. The exhaustion of the IPv4 address space forces the transition to IPv6. IETF has been considering the transition to IPv6 for several years. Main approaches include dual stacks, large scale Network Address Translation (NAT), and different forms of tunneling (6in4, 6to4, MPLS). The current strategy of IETF consists of encouraging experimentations involving existing approaches rather than working on new specifications of transition mechanisms. So, there is room for eventual patents that define specific parts of transition mechanisms. Tunneling seems to be the area in which much work may result in patents. Moreover, there is some need for mechanisms related to adaptation of IPv6 to upper layer services.

Sensor Networks and Internet of Things. This domain is in a phase of fast dynamic expansion. Many research activities focus on pushing IP to sensors, actuators, and communicating objects so that their constraints and physical world requirements call for new adaptation mechanisms. We believe that there are growing opportunities in this domain.

IPv6 in Mobile Networks, LTE and beyond. The integration of IP in mobile networks also opens new horizons for defining mechanisms that may be subject to patents. The complexity of mobile networks, the need for handling heterogeneous trafic with different QoS requirements, and guaranteeing high availability create a situation in which the basic functionality of IPv6 needs to be enhanced with additional mechanisms.

Virtualization. The recent trend towards Virtual Networks and Software Defined Networks may influence the way IPv6 will be used in the future networks. This active research area may also give rise to new patents.

4 Conclusion

The paper presents a set of patents related to the IPv6 technology. One aspect proper to IPv6 is the willingness of IETF to use license free algorithms and mechanisms. Despite this restriction, we can observe that several solutions are covered by patents—in particular, the mechanisms related to general concerns such as address allocation and issues related to access networks such as the detection of connectivity and termination. Finally, we have identified several areas subject to intensive research that seem promising for new patents: transition to IPv6, sensor networks and Internet of Things, IPv6 in mobile networks, and virtualization.

5 Acknowledgements

The work of G. Ferrari and A. Duda is funded by the European Community's Seventh Framework Programme, area ”Internetconnected Objects”, under Grant No. 288879, CALIPSO Project — Connect All IP-based Smart Objects. The work reflects only the authors' views; the European Community is not liable for any use that may be made of the information contained herein.

References

[1] S. Deering and R. Hinden, “Internet Protocol, Version 6 (IPv6) Specification,” RFC 2460, IETF Network Working Group, Dec 1998.

[2] S. Bradner, “The Internet Standards Process – Revision 3,” RFC 2026, IETF Network Working Group, 1996.

[3] S. Bradner, “Intellectual Property Rights in IETF Technology,” RFC 3979, IETF Network Working Group, Mar 2005.

[4] T. Narten, “Clarification of the Third Party Disclosure Procedure in RFC 3979,” RFC 4879, IETF Network Working Group, Apr 2007.

[5] S. Kawamura and M. Kawashima, “A Recommendation for IPv6 Address Text Representation,” RFC 5952, Internet Engineering Task Force (IETF), Aug 2010.

[6] C. Bao, C. Buitema, M. Bagnulo, M. Boucadair, and X. Li, “IPv6 Addressing of IPv4/IPv6 Translators,” RFC 6052, Internet Engineering Task Force (IETF), Oct 2010.

[7] C. Ding, “Apparatus, method and system for acquiring IPv6 address,” Patent US7958220B2, Huawei Technologies Co. Ltd., Jun 2011.

[8] P. Patel and H. S. Alkhatib, “Routing using global address pairs,” Patent US8351430, Microsoft Corporation, Jan 2013.

[9] J. A. Toebes, E. Levy-Abegnoli, and P. Thubert, “Migration to IPv6 using combination of globally significant and locally significant IPv4 addresses,” Patent US7764686B1, Cisco Technologies, Inc., Jul 2010.

[10] D. Farinacci, V. Fuller, D. Meyer, and D. Lewis, “The Locator/ID Separation Protocol (LISP),” RFC 6830, Internet Engineering Task Force (IETF), Jan 2013.

[11] P. FanXiang, W. HaiBo, Z. KeYao, Z. QingShan, Y. RenXiang, Z. XuDong, and J. YingLan, “Network service selection and authentication and stateless autoconfiguration in an IPv6 access network,” Patent EP1648134 B1, Alcatel Lucent, Dec 2007.

[12] P. FanXiang, W. HaiBo, Z. KeYao, J. Wei, Y. RenXiang, Z. XuDong, and J. YingLan, “Method and device for detecting connectivity termination within an internet protocol version 6 access networks,” Patent EP1641192 B1, Alcatel Lucent, Oct 2008.

[13] T. Narten, E. Nordmark, and W. Simpson, “Neighbor Discovery for IP Version 6 (IPv6),” RFC 2461, IETF Network Working Group, Dec 1998.

[14] J. T. Chapman, S. H. Desai, R. E. Droms, R. S. Krishnan, and M. Sudan, “Use of ipv6 in access networks,” Patent US7941512, Cisco Technology, Inc., May 2011.

[15] E.-H. Bae, S.-H. Choi, N.-J. Kwak, H.-N. Lim, and O.-S. Song, “Method and aparatus for performing handover between core network entities in a packet-swiched network,” Patent EP1744582 B1, Samsung Electronics Co., Ltd., November 2008.

[16] G. Shepherd and D. Farinacci, “Vpn services using address translation over an IPv6 network,” Patent US7483439 B2, Cisco Technology, Inc., January 2009.

[17] E. K. Jr., “Method and system for internet protocol address concatenation,” Patent US7653065 B2, Nortel Networks Limited, January 2010.

[18] V. Devarapalli and R. P. (Basavaraj), “Discovering a network element in a communication system,” Patent EP1759519 B1, Nokia Corporation, April 2010.

[19] G. F. Cortes, “Core network node selection in a mobile communication network,” Patent EP2425584 B1, Telefonaktiebolaget LM Ericsson, February 2013.

[20] P. R. Chitrapu, “Routing header based routing in internet protocol (IP)-cellular networks,” Patent US7043247 B2, Interdigital Technology Corporation, May 2006.

[21] C. Perkins, D. Johnson, and J. Arkko, “Mobility Support in IPv6,” RFC 6275, Internet Engineering Task Force (IETF), Jul 2011.

[22] J. Sundquist, “Provision of mobility for ipv4 traffic in an ipv6 network,” Patent EP1588534B1, Nokia Corporation, Jul 2007.

[23] C. Perkins, “RFC 2002 - IP Mobility Support,” RFC 2002, IETF Network Working Group, Oct 1996.

[24] J. Chen, J. Guan, D. Li, X. Pan, and L. Ping, “Method and system for fast handover in hierarchical mobile IPv6,” Patent EP1988665B1, Huawei Technologies Co., Ltd., Zhejiang University, Feb 2010.

[25] S. Thomson and T. Narten, “IPv6 Stateless Address Autoconfiguration,” RFC 2462, IETF Network Working Group, Dec 1998.

[26] H. Jung, S. J. Koh, and J. Y. Lee, “Fast Handover for Hierarchical MIPv6 (F-HMIPv6),” tech. rep., Internet Engineering Task Force (IETF), Apr 2005.

[27] Y. Han, “Method for reserving a new care of address (COA) in advance to achieve a fast handover under a mobile internet protocol version 6 (IPV6) environment,” Patent EP1473901B1, Samsung Electronics Co., Ltd., Jun 2007.

[28] J. Bachmann and K. Weniger, “Mobile IPv6 optimised reverse tunnelling for multihomed terminals,” Patent EP1739901B1, Panasonic Corporation, Jul 2012.

[29] J.-H. Kim, “Method and apparatus for providing gateway to transmit ipv6 packet in a wireless local area network system,” Patent US8036108, Samsung Electronics Co., Ltd., Oct 2011.

[30] S.-H. Park, “Header compression and packet transmission method in sensor network and apparatus therefor,” Patent US8149816B2, Samsung Electronics Co., Ltd., Apr 2012.

[31] A. S. Patel, V. J. Ribiere, P. Thubert, J.-P-Vasseur, and P. Wetterwald, “Routing operations using sensor data,” Patent US8149816B2, Cisco Technology, Inc., Jul 2012.

[32] Z. Liu, R. D. Day, and E. S.-J. Swildens, “Server failover using IPV6 mobility features,” Patent US8341295, Akamai Technologies, Inc., Dec 2012.

[33] E.-M. Levy-Abegnoli and P. Grossetete, “Secured IPv6 traffic preemption,” Patent US8281383, Cisco Technology, Inc., Oct 2012.

[34] D. Awduche, J. Malcolm, J. Agogbua, M. O’Dell, and J. McManus, “Requirements for Traffic Engineering Over MPLS,” RFC 2702, IETF Network Working Group, Sep 1999.

[35] R. Braden, L. Zhang, S. Berson, S. Herzog, and S. Jamin, “Resource ReSerVation Protocol (RSVP),” RFC 2205, IETF Network Working Group, Sep 1997.

[36] S. Herzog, “RSVP Extensions for Policy Control,” RFC 2750, IETF Network Working Group, Jan 2000.

[37] K. Nichols, S. Blake, F. Baker, and D. Black, “Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers,” RFC 2474, IETF Network Working Group, Dec 1998.

[38] S. Blake, D. Black, M. Carlson, E. Davies, Z. Wang, and W. Weiss, "An Architecture for Differentiated Services," RFC 2475, IETF Network Working Group, Dec 1998.