

The Benefits of IPv6 for the Mobile Internet

Table of contents

Executive Summary	3
Introduction	4
The Benefits of IPv6	4
Addressing	4
Security	6
Performance	6
Administration	7
Mobility	7
IPv6 in the Mobile Internet	7
IP in 3G Networks	8
Migration	8
Security Features	9
Efficiency Over the Air	9
Mobility	9
Abbreviations	11

Executive Summary

Ericsson was founded on the principle that communication is a basic human need, and this principle still guides us as we look to the future.

The two foremost trends in communication over the past decade have been the growth of mobile telephony and the Internet. In the near future, it will be more common to make a telephone call using a mobile telephone than a traditional fixed-line telephone. The Internet, and especially the World Wide Web, continues to revolutionise the way that people, businesses, and machines communicate.

We foresee that these two technology trends will combine to form the next major change in communication — the Mobile Internet — such that by the year 2003 there will be more Internet connections made from mobile devices than from fixed ones. New services will become available that are built on the concepts of personalization, mobility, location and security. Many devices will communicate over the Internet using built-in miniature mobile telephones. These devices are expected to number in the billions, and may be present in cars, vending machines, key rings, alarm systems, cameras and a multitude of other items as the cost of technology falls.

These changes will accelerate as third generation (3G) of mobile networks and services become available in the near future, allowing up to one hundred times more bandwidth than the wireless services we have today.

The Internet Protocol (IP) will form one of the cornerstones of these networks. Ericsson's vision is that all mobile users in the near future will be 'always connected and always online'.

Ericsson believe that IP version 6 (IPv6) is essential in making this vision real; IPv6 helps to solve many problems that will appear with the rapid growth of the

Mobile Internet. Tremendous opportunities will become available for service providers and network operators to create new business opportunities and to differentiate services.

IPv6 supports functions crucial to the deployment of scalable IP networks as a basis for new and exciting 3G services. Consequently, Ericsson is fully committed to introduce IPv6 in all of its products to provide seamless end-to-end services.

With long experience in cellular technologies and early pioneering work in IPv6, Ericsson is uniquely capable of combining IP technology and wireless networks to create the Mobile Internet.

Introduction

The rapid increase in the number of Internet users, combined with the expected growth in the number of wireless Internet devices requires a scalable and flexible IP technology to accommodate such fast growth (see Figure 1). IPv6 was developed by the Internet Engineering Task Force (IETF) to satisfy the requirements of the future Internet.

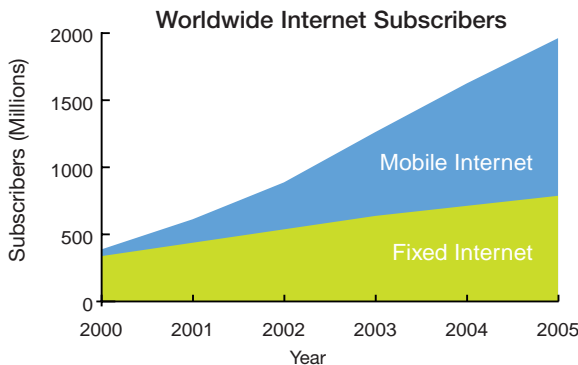


Figure 1 Rapid growth of fixed and mobile Internet subscribers

The feature of IPv6 that receives most attention is that it has a much larger range of available addresses than IPv4, but this is far from being the only benefit. In reality, IPv6 considers a wide range of capabilities and integrates a number of important features that have been treated as add-ons to IPv4.

Unsurprisingly, given IP's now venerable age, these features were not foreseen as being important when IP was originally conceived during the 1970s. Proponents of IPv4 often claim that the extensions made to it will serve quite adequately for some years yet. While a theoretical case can be made for this view when considering each feature in isolation, it is difficult to sustain this opinion when considering the broader picture, taking into account how these features interact. IPv6 then becomes the only complete solution available.

Always connected and always online

IPv6 is an essential technology to realise the vision of a large number of people being '*always connected and always online*', particularly due to the limited number of IPv4 addresses available. New services, such as multimedia, require globally unique addressing. IPv6,

with its very large address space, will guarantee a globally unique IP address for each device for many years to come.

Nevertheless, IPv6 hosts and terminals will need to inter-operate with IPv4 hosts and terminals for a long time. Therefore it is important to plan for IPv6 migration and coexistence of IPv4 and IPv6. The migration strategy must be based on business needs and benefits, for both network operators and their customers and ensure that both IPv6 and IPv4 can be used in routers, hosts and terminals and that appropriate interworking mechanisms between the two protocol suites are available.

The Benefits of IPv6

Wireless networks have very stringent requirements in terms of scalability, quality of service and security. IPv6 addresses all of these issues. Standardisation of IPv6 has reached a point where it is ready for commercial service and is being promoted through industrial forums of major operators and vendors.

The IPv6 architecture and design includes a number of attractive features that make it a valuable component of an IP-based 3G wireless network. These benefits can be grouped as:

- Addressing
- Security
- Performance
- Administration
- Mobility

Addressing

More addresses

Every online device or computer needs a globally unique IP address to connect to the Internet. When IPv4 was designed in the 1970s, it was difficult to foresee that its 4 billion unique addresses would ever be exhausted. However, the way in which IPv4 addresses have been allocated and the tremendous success of the Internet have made IPv4 addresses a scarce resource. This problem is particularly serious in certain areas of the world, for example Asia, where there are far fewer IPv4 addresses than in Europe and in the United States.

The limited number of IPv4 addresses is also an issue for those operators wishing to extend their businesses from mobile telephony to the Mobile Internet, as additional IPv4 addresses are now very difficult to obtain.

Demand for IP addresses is growing exponentially due to the Internet's evolution. Further draining the pool of IP addresses is the aggressive rollout of 'always connected' services and the proliferation of laptops, Personal Digital Assistants (PDAs), digital cameras, game consoles and telemetric devices.

Currently in the Internet, addresses are often shared between multiple connections, which helps to conserve addresses. This cannot be the case once persistent services become available, as each connection will rely on unique addresses. Today, many people have dial-up services with approximately one modem for each ten subscribers to the ISP, and hence 90% of the addresses are saved compared with 'always connected' services. In addition, corporate users of the Internet are commonly connected via translation devices that also conserve addresses by allowing many computers to share a single address. As there will probably be several permanently attached devices per person, it is obvious that IPv4 addresses will be exhausted in the near future. Some estimates are that this will happen before the end of 2005.

Current approaches to solving these issues in IPv4 networks, such as Network Address Translation (NAT), which translates between global and private IP addresses, introduce new problems of their own. For example, NAT makes it virtually impossible to deploy end-to-end security using IP Security (IPsec). NAT also eliminates the possibility of end-to-end conversational multimedia services, as these require unique IP addresses for any-to-any connections.

IPv6 allows 340 billion billion billion billion (3.4×10^{38}) unique addresses, which is enough to provide billions of addresses per person. Any device connected to the next generation Internet may therefore have a unique address.

Addressing Hierarchy

Due to the inefficient allocation of addresses, IPv4 suffers from limited route aggregation possibilities and thus very complex routing. The introduction of

Classless Inter-Domain Routing (CIDR) to IPv4 has allowed more aggressive route aggregation. This has helped to slow-down the growth of routing tables in the Internet's core. Such growth would otherwise cause performance limitations and management burdens. However, even this has not been enough to overcome the inefficiency created by the previous allocation of addresses, and there are now more than 100,000 routing prefixes that need to be handled in the IPv4 Internet core.

Having learnt an important lesson from the problems facing IPv4, IPv6 was designed from the start to provide a *hierarchical address structure*, allowing route aggregation and ensuring that the routing tables are kept small. Consequently, it provides a scalable address space that can be flexibly divided.

Figure 2 shows an example of how this hierarchy might be used in practice. The long-haul provider in the example shown uses a top-level route. The corresponding next-level route is assigned to an organisation, e.g. a service provider that connects to the long-haul provider. The site-level route is then used by the service provider to create its own local addressing hierarchy, for example to allocate pools of addresses to corporate customers or smaller service providers.

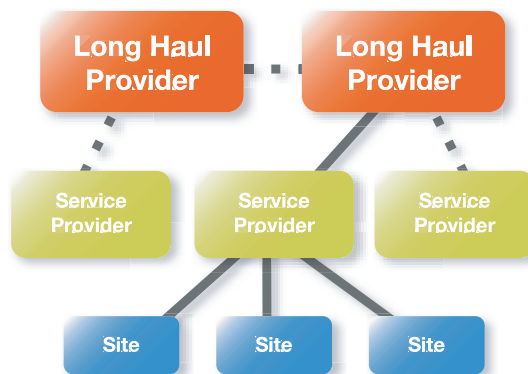


Figure 2 IPv6 unicast address allocation allows efficient route aggregation

Top level exchanges in the IPv6 Internet core will potentially only need to handle many fewer top-level routes, which may be an order of magnitude lower than the current IPv4 Internet core. This helps to simplify router design, and assists in improving their performance.

Security

IP security (IPsec) is built into IPv6 and can be utilised to protect both application and network specific data and signalling.

IPv6 provides end-to-end security mechanisms for authentication and encryption to all applications, without the need to integrate such support in all applications. The IPsec algorithms can be updated as improved cryptographic methods are developed.

The benefit of having the same security mechanisms available for use by all applications lies primarily in simpler administration of both security policies and security associations. Therefore, cost of ownership can be reduced compared with administering multiple security systems.

In addition, as IPv6 does not impose restrictions on end-to-end security, it should allow much simpler deployment of new, personalised services such as those that rely on secure transactions.

Performance

Quality of Service

Network operators can use the Quality of Service (QoS) mechanisms in IP to help provide a range of service packages with different performance characteristics and price levels.

The two main IETF standard protocol frameworks for supporting IP QoS, namely Differentiated Services (DiffServ) and Integrated Services (IntServ), apply in a similar way to both IPv4 and IPv6. Therefore, operators that adopt DiffServ or IntServ for IPv4 will find it relatively simple to migrate to services based on IPv6.

IPv6 allows future possibilities to enhance the Quality of Service mechanisms in IPv4 by using the 'flow label' field in the IPv6 header, whereby powerful, application flow-based resource reservation schemes and DiffServ enhancements can be added to complement the existing standards. It is worth noting that the flow label can be used even when the packet payload is encrypted, which renders other classification techniques, e.g. port numbers, to be unusable.

Finally, the need to use NAT in IPv4, due to address scarcity, is not necessary in IPv6. Therefore, the end-to-end performance degradation caused by NAT

processing is avoided, providing IPv6 with a corresponding QoS advantage.

Multicast

Multicast is a technique typically used when a stream of information, e.g. audio, video, financial data, or news, needs to be transmitted to many devices rather than to a single destination. This can help substantially with network efficiency as each packet is copied down through a tree-like structure, rather than being sent directly from the source to each destination point directly, as shown in Figure 3.

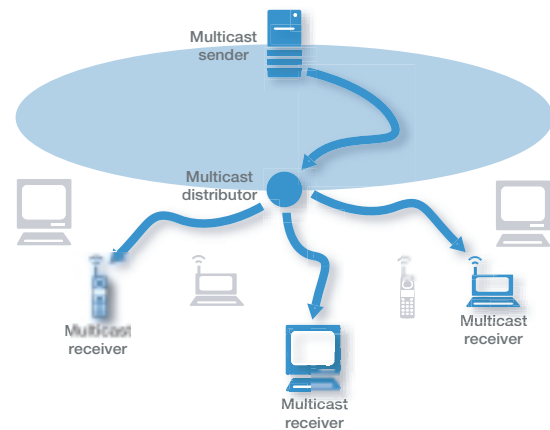


Figure 3 Multicast

This means that fewer packets are carried across the network, which improves bandwidth efficiency and reduces the resource requirements on network nodes.

The multicast support built into IPv6 extends the capabilities of IPv4 multicast by defining a very large multicast address range and expanding the scope identifiers that limit the degree to which multicast routing information is propagated.

Anycast

In addition, IPv6 introduces the concept of anycast services, which are not as well defined in IPv4. Anycast behaves somewhat similarly to multicast, except that each packet is sent only to the nearest reachable member of the group, rather than to all members.

Some of the benefits of anycast are that it can be used as a highly cost-effective method of discovering a server of given type, e.g. a DNS-server, and it can

provide redundant paths to a group of servers. In this case, if the route to the primary server becomes unavailable, subsequent sessions will automatically connect to the next server in the group. This is illustrated in Figure 4.

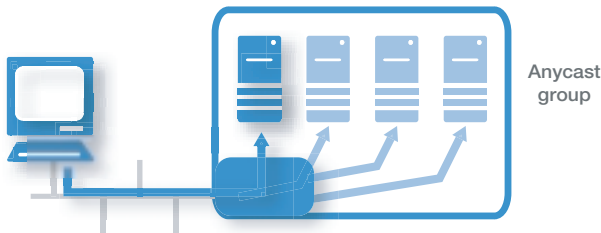


Figure 4 Anycast

Administration

IPv6 provides a number of features that help to simplify network administration. Address auto-configuration and automatic Domain Name Server (DNS) configuration will help to reduce the number of Dynamic Host Configuration Protocol (DHCP) servers that are widely used to dynamically allocate IP addresses in IPv4 networks. Therefore, there will be savings in the effort and cost involved in maintaining such servers.

IPv6 also provides capabilities for automated network renumbering which cannot be achieved in IPv4 networks. This allows for smooth network renumbering over a period without manual re-configuration of each router or host. This feature is extremely useful when expanding an existing network, merging two networks, or changing service providers.

Multi-homing provided by IPv6, i.e. where there is more than a single path to a destination, *can be a powerful technique for delivering reliable services*. This can be achieved by establishing simultaneous connections to two ISPs, hence providing a backup connection to the Internet when service is lost at one ISP. Multi-homing in IPv6 differs from IPv4 in that IPv6 allows the multihoming to be propagated to end hosts in a smooth manner, giving the possibility to place the responsibility of multi-homing on the end systems (e.g. hosts), rather than on a router.

Mobility

Mobile IP (MIP) was developed to manage a mobile device's IP mobility, and allow devices to move within the IP network (i.e. between IP sub-networks) with minimum interruption to connections. MIP can also be used to achieve seamless handovers between different access technologies, e.g. a cellular network and WLAN hotspot.

MIPv6 includes a number of advantages over the MIPv4 protocol such as route optimisation, which helps to avoid 'triangular routing'. This is described in more detail on page 9.

Due to the abundance of IPv6 addresses, MIPv6 eliminates the need for the additional mobility management functions that are required with MIPv4 (e.g. the use of a Foreign Agent). Furthermore, this allows network administrators to use security mechanisms, like ingress filtering, which prevent the use of invalid addresses within an operator's IP network.

IPv6 in the Mobile Internet

The introduction of IPv6 within the cellular world will significantly affect cellular network terminals, infrastructure, and applications by enabling a wide-range of new 'always connected and always online' services. These services, combined with the rapid growth in cellular devices, has led to the decision by the 3G Partnership Project (3GPP), to make IPv6 mandatory for all new services, of which the first is multimedia. The 3GPP provides technical documents for 3rd Generation Mobile systems.

Within this section, we will briefly consider the following aspects of using IPv6 in mobile networks;

- Migration
- Security features
- Efficiency
- Mobility

IP in 3G Networks

Within a 3G network, IP can be used for two purposes:

- User-level IP is used for communication between mobile devices and application hosts
- Transport-level IP is used for communication between network nodes in the cellular infrastructure

Figure 5 illustrates the use of IP in a 3G network.

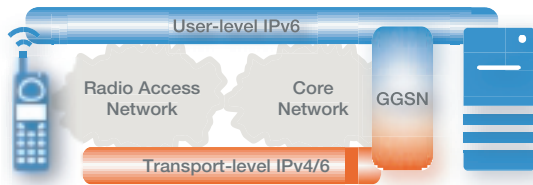


Figure 5 IP in a 3G network

The two layers can use different connectivity protocols e.g. IP versions. For instance, the transport-level can use IPv4, while the user-level provides the terminal with global IPv6 connectivity.

Migration

IPv4 and IPv6 will co-exist for a number of years. In the early stages of 3G networks, IPv4 will be widespread, with 'islands' of IPv6 connected via IPv4 networks. This situation is expected to change as more IPv6 capable devices are deployed, and IPv6 will gradually become the more widely deployed protocol.

One implication of this is that IPv6 networks need to be highly compatible with the installed base of IPv4 devices, and considerable attention has been paid to this issue as part of the standardisation work.

There are three main approaches to dealing with this issue: dual protocol stacks, translation, and tunnelling.

Dual Protocol Stacks

During the initial deployment of IPv6, it is expected that most terminals will implement *dual stacks*, i.e. both IPv4 and IPv6. In this instance, no translation is needed, as the terminal uses the appropriate IPv4 or IPv6 stack, depending on which host it is communicating with. This assumes that there are sufficient IPv4 addresses available; if this is not the case then translation is still required.

Translation

Some devices may only support IPv6. Since many existing networks and hosts are expected to run IPv4 for a long time, *translation* between IPv4 and IPv6 will be required to allow such IPv6 only devices to communicate with IPv4 only hosts.

For example, when an IPv6 terminal is communicating on the user level with an IPv4 host, an intermediate node is required to translate or re-establish the connection. These nodes are commonly known as Translators or Application Level Gateways (ALGs), and their use is illustrated in Figure 6.

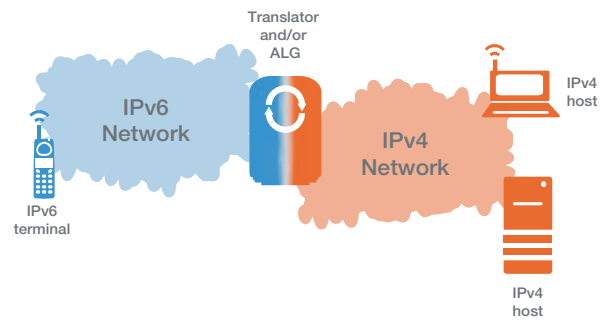


Figure 6 Translation

Tunnelling

Cellular operators may re-use existing IPv4 backbone networks while introducing IPv6 networks at the edges. For these IPv6 domains to communicate effectively on the transport level, tunnelling of IPv6 packets between intermediate IPv4 points in the network is required. Similarly, user level traffic also needs to be tunnelled over the existing IPv4 network. Both cases are illustrated in Figure 7.

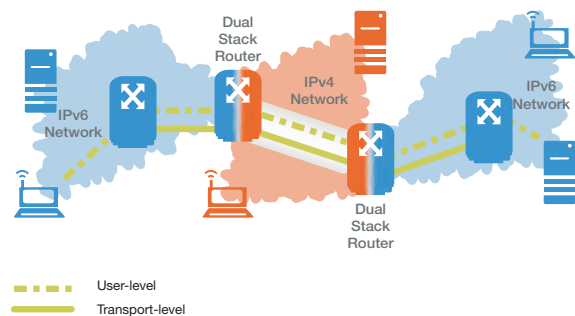


Figure 7 Tunnelling; connection of IPv6 sites via IPv4 networks

Tunnelling is highly appropriate when using native IPv6 terminals and services, and one or more IPv4 networks need to be crossed to achieve an end-to-end connection.

Tunnels may be established either dynamically; i.e. when the tunnel end point is selected based on analysis of the destination IPv6 address, or by manual configuration.

Security Features

Confidentiality of information is the major consideration that is relevant when exchanging data between terminals and hosts. This leads to the necessity to authenticate, authorise, and protect this traffic in an end-to-end fashion. For example, these security mechanisms would be appropriate where someone is using a mobile terminal to access a corporate Intranet via a Virtual Private Network (VPN).

IPsec has an inherent benefit in that it allows the ability to control the level of security offered to match the requirements of individual application flows.

Efficiency over the Air

IPv6 opens up new possibilities for the Mobile Internet. This involves the IP “all the way” concept, where the Internet Protocol is carried “end-to-end” from one mobile device to another. In wireless systems this means that IPv6 is carried over the air interface, with its high error rates and limited capacity.

The large header of IPv6 causes high bandwidth consumption. A solution that addresses this issue is Header Compression, which maintains end-to-end IP connectivity while reducing the size of the large IPv6 packet header over the error-prone and limited capacity air interface. Ericsson has been a major contributor to the work on Robust Header Compression (ROHC), through the ROCCO (RObust Checksum-based header COmpression) algorithm. ROHC is more robust and achieves higher compression than earlier algorithms, leading to better efficiency across the air interface.

The simple structure of the IPv6 packet header should allow improved performance and more efficient silicon implementation compared with IPv4, even though the header is twice as large.

Mobility

Consider the scenario in Figure 8 below, when travelling from left to right with a mobile PDA switched on. As the PDA moves, it is necessary to move the connection between either radio cells or IP areas. This is commonly called a handover.

The first handover is between Cells 1 and 2, which are both within IP Network A, so there is no IP handover. However, when the handover between Cells 2 and 3 takes place, an IP handover is also required as Cells 2 and 3 are connected to different IP Networks (A and B respectively).

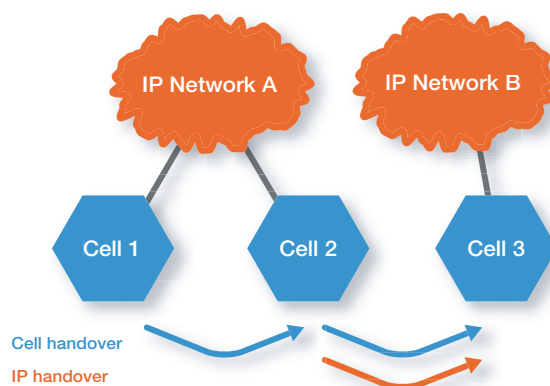


Figure 8 Mobility handovers

Mobile IP (MIP) is the most widely accepted solution for IP mobility. Mobility support is mandatory in every IPv6 implementation by the use of Mobile IPv6 (MIPv6). Since IPsec is in every IPv6 implementation, it is used to secure signalling between MIPv6 devices.

3G terminals are expected to implement a number of interfaces for use with different access networks. For example, terminals may also support other radio technologies like Bluetooth, Infrared, or WLAN. Assuming that those access technologies are connected to different access routers, a terminal's IP address may change when moving between those different media.

MIPv6 can be used to ensure seamless mobility and maintenance of ongoing connections. MIPv6 can also be used when roaming between different 3G networks, thus allowing an optimized route to be used to reach the device. This is illustrated in Figure 9.

white paper

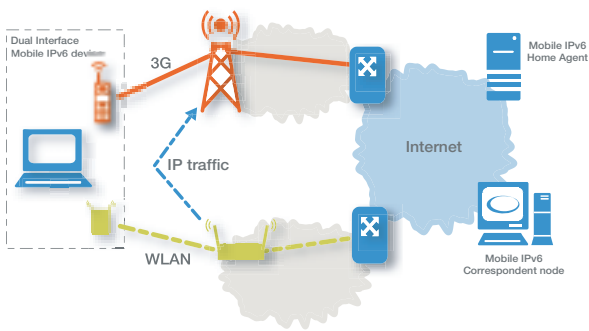


Figure 9 IP Roaming between different network interfaces

MIPv4 is currently supported within the 3GPP standards by the inclusion of the Foreign Agent capability in the Gateway GPRS Support Node (GGSN). Since no Foreign Agents are required in IPv6, MIPv6 is easier to deploy than MIPv4.

MIPv6 also provides an end-to-end mechanism for optimised routing within the network, so that triangular routing is avoided. Figure 10 illustrates this.

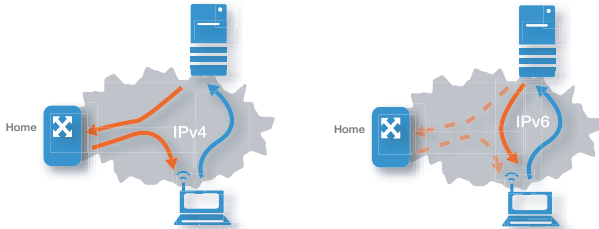


Figure 10 Triangular routing and route optimisation

The left picture shows triangular routing; data from the server to the PDA has to pass via the home network, as the server is only aware of the PDA's home address, not where it has roamed to in the network. On the right hand side, route optimisation has been used, and now the data from the server can be sent directly to the PDA. The optimised route is much more efficient, as the data is delivered with less delay, and uses fewer network resources since the data only travels across the network backbone once.

Abbreviations

3G	Third Generation Mobile Telecommunications	IPsec	IP security
3GPP	3G Partnership Project	ISP	Internet Service Provider
ALG	Application Level Gateway	LAN	Local Area Network
ATM	Asynchronous Transfer Mode	MIP	Mobile IP
CIDR	Classless Inter-Domain Routing	NAT	Network Address Translation
DHCP	Dynamic Host Configuration Protocol	PDA	Personal Digital Assistant
DNS	Domain Name Server	QoS	Quality of Service
GGSN	Gateway GPRS Support Node	ROCCO	RObust Checksum-based header COmpression
GPRS	General Packet Radio Service	ROHC	Robust Header Compression
IETF	Internet Engineering Task Force	UMTS	Universal Mobile Telecommunications System
IP	Internet Protocol	VPN	Virtual Private Network
IPv4	Internet Protocol version 4	WLAN	Wireless LAN
IPv6	Internet Protocol version 6		

Ericsson is shaping the future of Mobile and Broadband Internet communications through its continuous technology leadership. Providing innovative solutions in more than 140 countries, Ericsson is helping to create the most powerful communication companies in the world.