DELIVERABLE D6.2

IPv6 based secure communication

Title of Contract	Seamless Communication for Crisis Management
Acronym	SECRICOM
Contract Number	FP7-SEC-218123
Start date of the project	1st September 2008
Duration	44 months, until 30th April 2012
Date of preparation	30th November 2009
Author(s)	Aurel Machalek, Aldabbagh Ahmed, Vladimir Hudek, Oscar López, Saioa Ros, Ewa Adam, Mikel Uriarte, Shaun O´Neill, Wojciech Wojciechowicz, Stefan Kraxberger
Responsible for the deliverable	Aurel Machalek
Email	aurel.machalek@uni.lu
Reviewed by:	Oscar López, John Stoodley, , Ewa Adam, Shaun O´Neill
Status of the Document:	Final
Version	2.0
Dissemination level (select)	**PU Public**

Contents

List of Figures and Tables

1. Summary

The previous Deliverable D6.1 in WP6 called *Report on existing IPv6 based group call solutions* was theoretically based for the introduction of IPv6 in communication and maps existing communication technologies using IPv6. The deliverable D6.1 gave clear justification as to the benefits of IPv6 in communication techniques and especially in crises situations.

This Deliverable D6.2 has moved the theoretical base to the Secricom solutions. Simplifying the problem we have taken all technical modules developed until now for Secricom solutions and placed into an IPv6 environment. The result should provide answers for these questions:

- Are all modules working with IPv6?
- Is the IPv6 adding value and can it benefit the solution?
- How it can improve IPv6 security the solution?

This report will not only highlight best practices of using end to end security services brought in by IPv6 but implement IPV6 to Secricom technical solution.

Chapter 2 is devoted to secure communication using IPv6 protocol. The IPv6 is known technology but there is lack of experiences in securing IPv6 networks. The chapter gives overview to the security problem with IPv6 and advice for future development of Secricom solution. The second part of Chapter 1 clarifies mobility in IPv6 and security issues of mobile IPv6.

Chapter 3 is devoted to Partial modules of Secricom solution in IPv6 environment. PTT solution is followed by Secure Docking Module, Multi-Bearer Router and Monitoring Solution for Secricom project. This chapter answers whether it is possible to run IPv6 protocol over Secricom´s modules and identifies possible problems and solutions

Chapter 4 is devoted to Quality of Service especially focused for implementation QoS to Secricom solution. QoS scenario is described as well as QoS enabled architecture with QoS agents on terminal.

Chapter 5 describes in detail SIP protocol, components of SIP, SIP architecture and impact of SIP protocol on the Secricom communication model.

Chapter 6 is focused on the scenario aspects of the Secricom project. The Description of Work states that IPv6 technology will be part of the project demonstration.

From the Secricom Description of Work, D6.2 includes the following tasks:

T 6.3: PTT enhancements by IPv6

While T6.1 and T6.2 is devoted to examine existing solutions and the coexistence of QoS in heterogeneous IP-networks, T6.3 is devoted to the implementation of QoS-support, security mechanisms and group-services. This topic covers Chapter 3.

T 6.3.1: QoS (Capacity, Reachability, Delay)

If SIP is used together with IPv6, SIP is responsible for signaling and connection management. IPv6, on the other hand, has to take care of the actual PTT communication and routing. However, QoS is treated in both protocols:

1. QoS is inherently supported by the SIP-related real-time transport protocol (RTP), which is responsible for the real-time data-transport and QoS feedback.
2. QoS is provided by IPv6, where QoS is based on Flow Labels and Traffic Classes.

Thus, it is self-evident that this complex construction needs to be investigated to eliminate redundancies and to find the best possible configuration.

This topic is detailed clarify in the Chapter 4 and Chapter 5.

T 6.3.2: Security

In terms of PTT mechanism, IPv6 security mechanisms can be used for:

- Authentication against PTT agents
- Ensure integrity of voice payload and QoS signaling info
- Avoid known threats

Chapter 2 is focusing on this content.

Chapter 3 is taken partial modules used in the Secricom project and described the functionality in the IPv6 environment.

T6.4 Preparation for Demonstration and Dissemination

Chapter 6 is devoted to the scenario part of Secricom project which can be used during the planned demonstration.

2. Secure communication with IPv6 technology

2.1. Introduction

IPv6 implementations are relatively new to the market, and the software that has created these systems has not been field tested as thoroughly as their IPv4 counterparts. There is likely to be a period of time where defects will be found, and vendors will need to respond quickly to patching their bugs.

The early adopters of IPv6 technology are encouraged to go carefully and make sure that security is part of their transition plans.

This lack of IPv6 deployment experience of the industry causes a lack of experience in securing an IPv6 network. Not many IPv6 attacks exist or are publicly known, and there are few best practises for IPv6 security. However some sophisticated hackers are beginning to well understand IPv6, and they use it as back doors for their tools and they also use IPv6 within IPv4 to obscure attacks and bypass firewalls.

It is fair to say that current IPv6 Internet is not a big target for attackers. That is why is important to understand the issues with IPv6 and prepare the defences.

In general terms, IPv6 security architecture is not so different to IPv4 one.

Nevertheless, in IPv6, Mobile IPv6 and tunnels can change the perimeter concept into a fuzzier one, and greater use of end-to-end encryption is needed to secure the different communication flows.

A good approach to secure an IPv6 network is to have a security architecture that has a perimeter (or system boundary) and internal controls to not only mitigate the Internet threats but also the insider threats.

The Internet community continues to evolve IPv6 solutions. Nowadays, security risks can be mitigated by adequate training of the IT staff, by installing the correct protection mechanisms, by updating the security policies with the new security issues that IPv6 brings and by keeping IPv6 device up to date so that when a new IPv6 vulnerability appears the systems are protected.

2.2. IPSec

IPSec is a framework of open standards, from IETF, that define policies for secure communication in a network. In addition, these standards also describe how to enforce these policies.
Using IPSec, participating peers can achieve data confidentiality, data integrity, and data authentication at the network layer.

The base architecture for IPSec compliant systems is specified in the RFC 2401 and it says that "the goal of the architecture is to provide various security services for traffic at the IP layer, in both the IPv4 and IPv6 environments."
The main purpose of IPSec is to provide interoperable, high quality, cryptographically-

based security for IPv4 and IPv6. It offers various security services at the IP layer and therefore, offers protection at this and higher layers. These security services are, for example, access control, connectionless integrity, data origin authentication, protection against replays (a form of partial sequence integrity), confidentiality (encryption), and limited traffic flow confidentiality.

IPsec is a mandatory component for IPv6, and therefore, the IPsec security model is required to be supported for all IPv6 implementations in near future. In IPv6, IPsec is implemented using the AH (Authentication Header) and the ESP (Encrypted Security Payload) extension header. Since at the present moment, IPv4 IPsec is available in nearly all client and server OS platforms, the IPSec IPv6 advanced security can be deployed by IT administrators immediately, without changing applications or networks.

In IPSec a Key sharing mechanism will be needed. Current work is being made in the development of the new version of the IKE (Internet Key Exchange) protocol, the IKEv2.

Nevertheless IPSec has some issues to resolve yet.

Even with IPSec, there are many threats which still remain issues in IP networking. Though IPSec is mandatory in IPv6, the same issues with IPSec deployment remain from IPv4, as configuration complexity or key management.

Although IPv6 provides fundamental technology to prevent sniffing with IPSec, it does not provide any simplification for the key management issues that have proved to be challenging.

2.3. Secure Neighbor Discovery Protocol

IPv6 nodes use the Neighbour Discovery Protocol (NDP) for Neighbour Discovery (ND), Address Auto-configuration, Router Discovery (RD), Neighbour Un-reachability Detection (NUD), Address Resolution, Duplicate Address Detection (DAD), Redirection etc. If NDP is not secured, it is vulnerable to various attacks

On one side, the NDP specifications emphasize the use of IPSec to protect NDP messages. IPSec AH can be used with NDP messages to enhance security. Also, the hosts can verify through AH that Neighbour Advertisements and Router Advertisements do contain proper and accurate information.

On the other side, Secure Neighbour Discovery (SEND) protocol is designed to encounter the threats to NDP.

In the following lines, SEND protocol options are shown:

- **Cryptographically Generated Addresses (CGA) Option:**

The CGA ensures that the sender of an NDP message is the owner of the claimed address. Before claiming an address, each node generates a public-private key pair and the CGA option verifies this key

- **Timestamp Option**

The Timestamp option provides replay protection and ensures that unsolicited advertisements and redirects have not been replayed.

- **Nonce option**

The Nonce option protects messages when used in solicitation-advertisement pairs. It ensures that an advertisement is a fresh response to a solicitation sent earlier by the node.

- **Certification Path Solicitation:**

Authorization is provisioned for both routers and hosts with routers getting certificates from a trust anchor and hosts getting configured to authorize routers. Separate certification path solicitation and advertisement messages are used to know the certification path to the trust anchor. Hosts will send the Certification Path Solicitations.

The next table counters the threats encountered by SEND:

Threats	SEND countermeasures
Neighbour Solicitation/Advertisement Spoofing	SEND requires the RSA Signature and CGA options to present in solicitations-
Neighbour Unreachability Detection Failure	SEND requires a node responding to Neighbour Solicitations probes to Neighbour solicitations probes to include an RSA Signature option and proof of authorization to use the interface identifier in the address being probed.
Duplicate Address detection DoS Attack	SEND requires including an RSA Signature option and proof of authorization in the Neighbour Advertisements sent as responses to DAD.
Router Solicitation and Advertisement Attacks	SEND requires Router Advertisements to contain an RSA Signature option and proof of authorization.
Replay Attacks	SEND includes a Nonce option in the solicitation and requires the advertisement to include a matching option.

Table 1 - SEND countermeasures

2.4. Threats

In current deployments IPv6 makes some things better/worse/different, but no more or less secure than IPv4. Security issues in IPv6 are not better than in IPv4, just different.

The threats that are exposed below are divided in two main sections. The first one will outline attacks that significantly change as a result of IPv6, and the second summarizes attacks that do not fundamentally change.

2.4.1. Attacks with new considerations in IPv6

- Reconnaissance: the ping sweeps and the port scans in IPv6 will be much more complicated to perform due to the amount of possible addresses. But there are ways of discovering addresses, to perform the scan over them: known multicast addresses (all-nodes, all-routers…), to compromise a DNS server to obtain its device cache, the configuration of predictable addresses by the network administrator (based on the IPv4 or the MAC addresses) or to access the neighbour caches of a compromised router.
  - On one side, the difficulty of discovering the devices hinders the hacker attacks. But by the other side, it also makes it difficult for the administrator to control the network, so it will be necessary to develop new discovering techniques.
- Unauthorized access: This refers to the class of attack where the adversary is trying to exploit the open transport policy.
  - IPv6 Best Practices: IPSec may enable easier host access control.
- Layer 3-Layer 4 Spoofing: It is the ability for an adversary to modify its source IP address and the ports they are communicating on to appear as though traffic initiated from another location or another application. With this technique attacks as DoS, spam, worms, viruses, etc are performed. In IPv4 these attacks are more difficult to track down. However, in IPv6, addresses are located in a hierarchical way, so it is easier to track the source of the attack.
  - IPv6 Best Practices: Filtering in the ISP would help a lot to reduce the range of spoofed addresses.
- Fragmentation: The first purpose is to use fragmentation as a means to evade network security devices, such as NIDs or firewalls. The second purpose of the attack is to use fragmentation or other header manipulation to attack the networking infrastructure directly.
  - IPv6 Best Practices: In IPv6 the minimum MTU is 1280 bytes, so the network devices might drop any packet smaller than this size, except if it is the last fragment. Devices will also have to deny fragments addressed to an intermediate network devices, as those are not allowed to perform the fragmentation. It can occur that if the IPv6 packet has a lot of extension headers, the first fragment won't have included the transport layer header and this will have to be taken into account in the network devices not to drop this kind of packets.
- Broadcast Amplification Attacks (smurf): These types of attacks are commonly referred as "smurf" attacks. They are a DoS tool that takes advantage of the ability to send an ICMPv6 echo-request message with an IPv6 multicast destination address and a spoofed IPv6 source address. All the destination nodes respond to the spoofed source address and flood the victim with ICMPv6 echo-reply messages.

  - IPv6 Best Practices: Nodes must be configured not to generate respond ICMPv6 messages to a message with a multicast destination address and to reject all the messages with multicast source address. It will be necessary to pay attention to allow "packet too big" and "neighbour discovery" ICMPv6 messages.

- Viruses and worms: Lots of the IPv4 viruses have not changed, such as those which affect to the mail service or to the removable devices. In IPv6, worms are affected in their spread ability as they are not able to find new hosts to infect. Worms would be able to use the neighbour caches, DNS repositories… to discover addresses and continue spreading, and in dual stack nodes they could spread over IPv4.

  - IPv6 Best Practices: It will be necessary to discover techniques for tracking the attacks and to use IDS mechanisms and anomaly detectors with IPv6 support. It will also be necessary to maintain the systems up to date in software patches and antivirus.

- Neighbour discovery attacks: These attacks attempt to subvert the host initialization process or a device that a host accesses for transit. These attacks try to get end hosts to communicate with an authorized or compromised device or to be configured with incorrect network information. Those attacks correspond with the ARP and DHCP attacks in IPv4.

  - IPv6 Best Practices: To use Secure Neighbour Discovery (SEND).

- Routing Header: The routing attacks focus on disrupting or redirecting traffic flow. Thanks to the Routing Header, it is possible to make the packet pass through a list of intermediate nodes before arriving to the destination (that means it is possible to force the route of the packet). It would be even possible to create the ping-pong effect between two nodes in an indefinite way. This can cause DoS attacks. Besides, final nodes are forced to accept the routing headers, so this could be used to avoid the security policies.

  - IPv6 Best Practices: By one side, the Routing Header type 0 has been declared deprecated for avoiding this problem. By the other side, it will be necessary to avoid final nodes to resend packets with routing extensions.

2.4.2. Attacks with strong IPv4 and Ipv6 similarities

- Sniffing: This type of attack involves capturing data in transit across a network. And it is possible for the attacker to determine login credentials or view sensitive information in plaintext protocols.

  - IPv6 Best Practices: To use IPSec.

- Application Layer attacks: These attacks refer to all the attacks performed at the Layer 7 of the OSI model.

  - IPv6 Best Practices: Even assuming the worldwide implementation of IPSec and that a given connection can be cryptographically protected, there is

nothing to stop an application layer attack from traversing the encrypted link and causing the same damage as if it were in the clear.

- Rogue Devices: Rogue devices are devices introduced into the network that are not authorized.
  - IPv6 Best Practices: To use IPSec.
- Man-in-the-middle: The IPv6 header, and also the IPv4 header, doesn't have security mechanisms, so they are based in IPSec. This makes them vulnerable to the man-in-the-middle attack that could affect the key sharing protocol IKE.
  - IPv6 Best Practices: It is working in a newer version of this protocol, IKE2.
- Bogon filtering: "Bogon" is the name given to an IP packet that belongs to an area of reserved addresses that are not assigned yet. As in IPv4 almost all the addressing space has been already assigned, it is easier to block the bogons than allowing the no-bogons. On the other hand, in IPv6 only 3 TLAs (Top Level Aggregator, it is a field of the prefix of the IPv6 addresses) are assigned, so the ACLs will only allow these three ranges and will block the rest.
  - IPv6 Best Practices: The ACL filtering does not avoid the address replacement, but it reduces the range of possibilities.

DDoS (Distributed Denial of Service): This type of attacks leaves a set of geographically dispersed systems without the ability of offering a service. This attack is performed by means of a set of compromised devices that are linked among them by the Internet, and they act as robots of the hackers. Hackers force all the "robots" to send traffic to the victims, leaving them without resources. In IPv6, as the amount of addresses is much bigger, the attack could have huge dimensions.

2.5. *Security issues in transition mechanisms*

The migration to an IPv6 Internet will not be achieved overnight. IPv4 and IPv6 will have to coexist for several years. Several mechanisms have been developed to enable communication during this transition phase. The transition techniques are listed below:

- Dual Stack: The nodes have two protocol stacks (IPv4 and IPv6) enabled, and use IPv6 to contact IPv6 nodes and IPv4 to contact IPv4 nodes.
- Tunnels: Hosts and routers send and receive IPv6 packets using an overlay network of tunnels established over an IPv4 network.
- Protocol Translation: A protocol translator acts as an intermediary between IPv4 and IPv6 worlds. The address and the header of the packet are translated to allow the communication between IPv6 only nodes with IPv4 only nodes.

In this section a little review of these mechanisms is going to be made, and the security vulnerabilities related to them are going to be described, including an explanation of the applicable mitigation techniques.

2.5.1. Dual Stack

In dual stack, all hosts as well as network devices run both IPv4 and IPv6 stacks. Both versions of IP can safely coexist on the same network as because each network has a specific Layer 2 Ethernet type, 0x0800 for IPv4 and 0x86dd for IPv6. The value in the Type field for Ethernet informs the node which Layer 3 protocol follows in the Ethernet frame. Above the data link layer, the transport protocols (User data protocol [UDP] or Transmission Control Protocol [TCP]) are unchanged and run identically over IPv4 and over IPv6. On the top, the applications are usually not aware of the underlying network layer, except for logging the remote IP address or for authorization based on IP addresses.

A small issue of running dual stack is the increased memory consumption in routers because they need to have two routing tables, as well as some slight CPU increase I routers (two router protocols are usually required, one for IPv4 and the other one for IPv6) or in the host kernels (some timer need to be duplicated).

In the following lines, dual stack vulnerabilities are described.

- IPv6 latent threats: Those are IPv6 existing threats waiting to be activated. The main one is that IPv6 is enabled by default in several recent operating systems (notably Microsoft Vista and some Mac OS X and Linux versions), and systems might try to connect to the IPv6 Internet without explicit configuration by the user. If security administrators are not aware of this fact and there is no security policy or IPv6 security protection implemented, they are running the risk of attack. Even if a network does not run IPv6, dual-stack hosts are open to local IPv6 attacks. In this case the scope of the attack is limited, as the attacker must be Layer 2 adjacent to the victim. This attack will only be successful if the victim has no personal IPv6 firewall and if the Network Intrusion Detection System (NIDS) does not support IPv6.

Mitigation Techniques: To have a personal IPv6 firewall correctly configured. It could also be possible to disable IPv6 support or to block all the IPv6 traffic.

2.5.2. Tunneling

As said before, one of the transition mechanism used in the coexistence between IPv4 and IPv6 is the tunnelling. In the next section, the security issues in the tunnels are going to be listed, but before this, a brief introduction to the tunnelling mechanisms and the different methods of performing it will be made.

A tunnel is a bidirectional point-to-point link between two network end-points. Data is carried through the tunnel using a process called encapsulation in which IPv6 packet is carried inside an IPv4 packet, using IPv4 as a Data Link layer regarding to IPv6 packet transport. The term tunnelling refers to a way of encapsulating one version of IP in another, so packets can be sent over a backbone that does not support the encapsulated IP version.

Both end-points of the tunnel should be dual stack. The "Protocol" field of the IPv4 header would be filled in with the 41 value that indicates that the packet payload is IPv6 traffic.

Tunnels add overhead in terms of packet size and operation procedures. This is the reason why this approach is not the preferred one, but dual stack mechanism. Therefore, the tunnel approach might be the only practical option for some years until IPv6 becomes ubiquitous.

There exist several types of tunnels, classified by the method used by the encapsulating node to determine the tunnel end-point address.

- Manually Configured Tunnels: The end-point address is determined by the configuration information that is stored in the encapsulating node.
- Automatic Tunnelling: The end-point address is determined thanks to the IPv4 address embedded in the IPv6 packet that is going to be encapsulated, in an automatic way.
- IPv4 Multicast Tunnelling: The end-point address is determined by means of the neighbour discovery.

In each of these tunnel categories it is possible to distinguish different types of tunnels as well, and they will be listed in the following lines.

- Manually Configured Tunnels:
  - 6in4 tunnels: These tunnels simply encapsulate a complete IPv6 datagram inside an IPv4 packet. The tunnel end-point addresses are determined by the configuration information that is stored at the encapsulating end-point. The router at one end sends the IPv4 packet with its own IPv4 address as the source address and the IPv4 address of the router in the other end as the destination. This tunnelling method is used for interconnecting IPv6 sites, but only when a few amount of tunnels are required.
  - GRE Tunnel: This type of tunnel provides the service for implementing any point-to-point encapsulation design. Each of the tunnel end-points requires configuration. The IPv6 traffic is transported over the GRE (Generic Routing Encapsulation) protocol. GRE Tunnels are used not only for IPv6 packet encapsulation, but also for IPv4, Ethernet frame and so on. The kind of encapsulated protocol is indicated in the GRE header.
- Automatic Tunnelling:
  - 6to4 Tunnel: It is used for inter-site communications, that is, it communicates IPv6 sites over IPv4 networks. It is a router-to-router tunnel. Each site will have a 6to4 router (it will be a dual stack router) and a prefix consisting on 2002::/16 + IPv4 address of the 6to4 router of that site. Because global IPv4 addresses are unique, this also makes the IPv6 prefixes unique. Router advertisement can be used by the 6to4 router to advertise this prefix to the inside IPv6 networks. There is no need to specify the IPv4 address of the tunnel destination because the IPv6 destination address already includes this IPv4 address. It can occur that the traffic would have to travel over native

IPv6 networks to reach its destination, in this case special gateways or relays will be required to cross those networks.

- ISATAP: Intra-Site Automatic Tunnel Addressing Protocol. It connects isolated dual stack hosts to an Ipv6 network. The isolated host will be configured with the set of IPv4 addresses of the possible ISATAP routers, this will be the Potential Router List (PRT), and will send IPv6 packets to the ISATAP router directly encapsulated inside an IPv4 packet using protocol 41. By one hand, the ISATAP router will provide the host with the IPv6 prefix that it should use in the IPv6 network. By the other hand, the interface identifier will consist on 0000:5EFE + the 32 bits of the host's IPv4 address expressed in hexadecimal notation. And that is how the isolated node will be able to auto-configure its IPv6 address.

- Teredo Tunnel: it is an automatic host-to-host tunnel designed to connect hosts that are located behind Nat with native IPv6 networks. It tunnels the IPv6 packets over UDP instead of over protocol 41. In the process several devices will take part: The Teredo client (the host behind the NAT), the Teredo relay (it will be in charge of the encapsulation and decapsulation) and the Teredo server (it is a registration server for clients and relays, through which clients will discover the relays and vice versa). The client makes a request to the Teredo server over the 3544 UDP port and this one sends to him an IPv6 address formed in a special way (this address will be included in the range 2001:000::32 and based on its public IPv4 address and the used port). The Teredo server and the relay talk over IPv4, and the relay acts as IPv6 router between the Teredo service and the native IPv6 networks.

- Tunnel Broker: It is a semiautomatic host-to-router tunnel that is used when a device in an IPv4 only network needs IPv6 connectivity. In this mechanism take part the client (host which needs Ipv6 connectivity), the tunnel broker (it provides to the client a web interface and acts as an intermediary between the client and the server) and the tunnel server (it will provide to the client with the IPv6 address and a script for creating the tunnel).

- IPv4 Multicast Tunnelling:

  - 6over4 Tunnel: It is also known as IPv4 Multicast Tunnelling. It is designed to transmit IPv6 packets between dual stack nodes on top of a multicast-enabled Ipv4 network, so the IPv4 network must have the multi-diffusion capability. It uses IPv4 as the link layer for IPv6. It allows performing neighbour discovery for obtaining the end-point addresses and it doesn't require any special prefix.

If the network designer does not consider IPv6 tunnelling when defining security policy, several security issues will appear.

On the following paragraphs, there is a list of some of the main security problems that the tunnelling mechanism has to face up. By one hand, the tunnelling techniques basically

have no built-in security, no authentication, no integrity check and no confidentiality. This translates into several generic threats applicable to all tunnelling mechanisms.

- Tunnel Injection: An attacker can inject traffic in a tunnel by pretending to be a legitimate user, by spoofing the external IPv4 and the internal Ipv6 addresses.
  - Mitigation Technique in Manually Configured Tunnels: In this case there exists enough configuration information to raise the security of the tunnel. It is possible to protect the Configured Tunnels by combining IPv4 source address checking and filtering, antispoofing techniques and IPSec.
  - Mitigation technique in Automatic Tunnels: In this case, the tunnel end-points must accept encapsulated traffic from anywhere in the IPv4 world. So, besides the use of IPSec, little can be done to reject illegitimate traffic.
- Tunnel sniffing: A spy located in the IPv4 path of the tunnel can sniff the tunnelled IPv6 packets and get access to the content of a conversation.
  - Mitigation Technique: In Manually Configured Tunnels it is possible to use the same security mechanisms as in the previous case, that is, the combination of IPv4 source address checking, antispoofing techniques and IPSec.
- Another problem in the tunnels is that if firewalls and IDSs are not dual stack, they won't be able to handle this type of packets. If the device only supports IPv4, when receiving an IPv6 packet encapsulated over IPv4, it will only be able to distinguish that the IPv4 packet transports the protocol 41, or UDP traffic in the case of the Teredo tunnel. And if the device only supports IPv6, it won't be able to see anything.
  - Mitigation technique: Firewalls and IDSs should support both IPv4 and IPv6, or the tunnels should be ended on or outside the security boundary, that is, before crossing these devices (in the case they only support IPv6).

By the other hand, there also exit tunnel vulnerabilities particular for a type of tunnel. Those threats are shown below.

- In the 6to4 tunnels, any 6to4 router must accept packets coming from other 6to4 router, from a relay or from a native IPv6 router. This can be exploited by malicious nodes for performing DoS attacks, service theft and unauthorized access.
  - Mitigation Technique: The relays must drop any packet arriving by the native IPv6 interface and having a source IPv6 address of the 6to4 type; any packet arriving by the 6to4 interface and having a source IPv6 address not of the 6to4 type; any packet whose source IPv4 address doesn't match with the address embedded IPv6 address.
  - IPSec in 6to4 tunnels can only be used when 6to4 routers and relays are within the same administrative domain because IPSec requires some shared configuration.

Some tunnels, as 6to4 or ISATAP, give well-known values to their network prefixes and they base the interface field value on the IPv4 addresses. That is why they might be predictable and easy to scan.

2.5.3.Protocol Translation

Network Address Translation-Protocol Translation (NAT-PT) allows native IPv6 hosts to communicate with native IPv4 hosts and vice versa. The NAT-PT device is at the boundary between an IPv4 and an IPv6 network. Each NAT-PT device has a pool of globally routable IPv4 addresses to be assigned dynamically to IPv6 nodes. Packet headers are transparently translated as they cross between IPv4 and IPv6 networks.

In the following lines, dual stack vulnerabilities are described.

- NAT-PT breaks end-to-end IPv6 security. There is no way to configure an IPSec tunnel between and IPv4 only host and an IPv6 only host.
- Reflection attacks: It is a method of attacking a challenge-response authentication system that uses the same protocol in both directions. The operating mode of the attack is to trick the target into providing the answer to its own challenge. A host in the IPv4 side sends a spoofed packet with a forged IPv4 source address and the final destination on the IPv6 side sends a reply to the spoofed address. A similar attack can be performed from the IPv6 side.
- Pool depletion attack: It is a DoS attack. A rogue IPv6 user sends several outbound requests (each with a different spoofed address) to some IPv4 servers, and each request consumes an IPv4 address from the NAT-PT pool. After several of those requests, the pool is depleted, and no further requests are accepted.
    - Mitigation Technique: To enforce rate limiting within the NAT-PT device. This attack can also be prevented by enforcing strict antispoofing techniques in the network up to individual hosts, with mechanisms such as IP source guard.

IPv6 to IPv4 translation and relay techniques can defeat active defence trace back efforts hiding the origin of an attack.

NAT-PT has been deprecated by the IETF due to its technical and operational difficulties.

2.6.Mobility in IPv6

The great evolution of portable devices enables their users to function while mobile as if they were in their home location. The mobile devices must be able to connect to a variety of networks as they roam and hop from one network medium to another.

2.6.1.Mobile IPv6 and its Security Issues

Mobile IPv6 (MIPv6) is a protocol that will provide seamless communications while IPv6-enabled device roams among connected networks.

The following definitions are important for understanding the basis of MIPv6:

- Access Router (AR): Router that provides internet access to the a Mobile Node
- Care-of Address (CoA): IP address of the Mobile Node at its current attachment point
- Correspondent Node (CN): An IPv6 device that is communicating with the Mobile Node via IP
- Home Agent (HA): Host on the Home Network that enables the Mobile Node to roam
- Home Network (HN): Network that a Mobile Node belongs to when it is no roaming. The HA will belong to the HN.
- Home Address (HoA): The Mobile Node address in the HN. CNs will send the packets to the HoA of the MN.
- Mobile Node (MN): An IP device capable of changing its attachment point to the Internet while maintaining higher layer connectivity through mobility functionality.

The MN will have two addresses, the HoA and the CoA. When a MN is in a foreign network, it obtains a local address, that is, the CoA. Then the MN sends the CoA to its HA for binding. Once binding is complete, the HA intercepts packets that arrive for the MN's HoA and forwards them to MN's CoA via a tunnel. Reverse traffic follows the same path through the tunnel to the HA for forwarding via standard routing on the Internet. As the MN moves to different foreign networks, it sends binding updates with its new CoA.

In the Figure 1 below the Mobile IPv6 Communications Model is depicted.

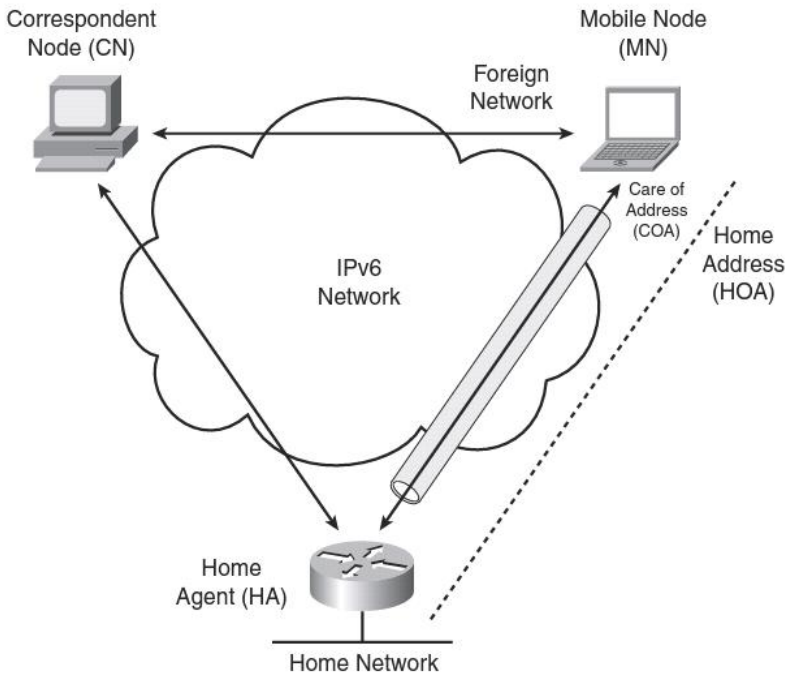

Figure 1 – Mobile IPv6 Communication Model

MIPv6 uses multiple IPv6 extension headers, such as, Mobility Option Header, Destination Option Header, several ICMPv6 messages and Type 2 Routing Header (RH2) for signalling.

Unfortunately these mobile devices are easy targets for attackers because they lack the security protections they had in their organization's internal networks.

In this section, the threats against the MIPv6 protocol will be shown, as well as some mitigation techniques for those vulnerabilities.

In the following paragraphs the threats linked to MIPv6 will be listed. Nodes that used to be inside an organization's network are now mobile and outside the protected zone, which introduces security risks.

- Protecting Mobile Device software: Historically devices such as smart phones were not in IP networks, so these devices are now exposed to new threats on an IPv6 internet, as they are not protected by a centralized firewall. Moreover, the service providers might protect the IPv4 connectivity of the devices, but leave the IPv6 connectivity unprotected.
  - Mitigation Technique: The device should provide its own security mechanism.
- Rogue Home Agent: An attacker could set up a rogue HA and thus be in the middle of all mobile communications, this would be an insider attacker.
- Mobile Media Security: Typically wireless network do not have the same assurance against eavesdropping than wired networks, unless some type of encryption is used. MIPv6 is vulnerable to the RF signal being intercepted by an attacker, and the risk increases if the MN roams to a foreign network. So if Layer 1 or Layer 2 communication medium is insecure, Layer 3 communication are also vulnerable.
- Man-in-the-middle attack: For performing this threat the attacker requires to have knowledge of the IPv6 addresses being used by the CN, the MN or the HA, so that he can capture all the important packets and influence on the communications. This can be difficult unless the attacker is close to any of these nodes or unless the attacker in present along the traffic path.
- Connection Interception: All MIPv6 signalling and data communications take place in the clear, and in this case the risk is bigger due to the inherently insecure wireless media. If the addresses of the CN, MN HoA, MN CoA or HA are identified by sniffing packets, an attacker could use this information for malicious activities and future attacks. The connection interception threat involves an attacker creating falsified packets to impersonate either the CN or the MN. The attacker will try to infiltrate the MIPv6 signalling to create fake bindings, making either the HA or the CN believe that the attacker in the valid MN. The attacker would try to act as a MN for a host that is not at home.
- Spoofing MN-to-CN bindings: The goal of these types of attacks is to create a man-in-the-middle attack, where the attacker could either eavesdrop or perform session hijacking. If the attacker knows the IPv6 addresses of CN and MN ahead of time, the attacker can potentially put together the two connections and observe the traffic being sent between the two.

- There are also attacks that involve creating a DoS attack through crafted packets.

On one hand, it would be possible to mitigate some of these attacks by using IPSec with MIPv6. There exist weaknesses in MIPv6 when the messages are not authenticated and their contents are not encrypted. Use of IPSec can prevent eavesdropping of the traffic being carried by MN, by authenticating the MNs allows to contact the HA. It can also protect the signalling traffic exchanged between the MN and the HA. It is clearly stated in the RFC 3775 that IPSec is a requirement for communications between the MN and the HA, that is, a mandatory IPSec ESP transport mode tunnel is set between both nodes. The CN communication is not secured.

IPSec provides a way to help secure MIPv6, but many of the smaller devices might not be capable of running it. For example mobile phones can lack the computational capability to perform the cryptographic calculations in software. Fortunately the functionality in mobile devices will continue to increase.

Another difficulty for the wide scale deployment of Internet-based IPSec is the lack of a global public key infrastructure (PKI). Nevertheless, IPSec is only required for the communications between the MN and the HA, and as this both nodes are part of the same organization they can use a pre-shared key or use an internal PKI to validate their authenticity to each other.

Another possible mitigation technique for the threats listed before could be filtering the communications between the remote nodes and the HA, by using Access Control Lists (ACLs). To achieve it, signalling packets should be protected to help secure the control traffic, and the data exchanged between the MIPv6 devices should be limited.

Filtering can be difficult in MIPv6 networks due to the added extension headers for mobility. Filtering systems need to look inside the payload and interpret the source/destination addresses, which can be different than the physical IP addresses being used by the MN.

MIPv6 filtering should be done in the firewall of the home network, in the CN, in the MN and in the HA. The important thing to notice is the message types that are required among these three MIPv6 nodes for the protocol to function properly. Restricting the packets any further would result in failed communications between the CN, MN and HA.

The home network should keep track of the MNs, locally and remotely, and it should expect messages from the CNs and forward them to the MNs. It will be necessary to configure the home network perimeter to prevent rogue MNs from joining the HA and these fake devices gaining access to the home network. In the following lines the packets that should be allowed by the ACL in the firewall are listed:

- RH2 packets coming from designated HAs and authorized CNs
- Destination Option Header type 201 packets, which indicate to the recipient that the packet was originally sourced from the MN's HoA.

- Mobility Extension Header packets, used for most signalling traffic and required for creating the MN and the HA bindings.
- MIPv6 special ICMPv6 messages that are used by the MN to discover information from the HA.

According to the filtering at the CN, as long as the protocols between the CN and the MN are acceptable to the firewalls along the path, the CN needs no special filtering.

Finally, to harden the HA it is possible to restrict the foreign links that an MN can have, to limit the maximum number of binding cache entries held by the HA and to adjust the binding lifetime or the refresh interval.

2.6.2.Network Mobility: NEMO

While in Mobile IP it is the end systems which change the point of attachment, in Network Mobility (NEMO) it is the entire network who changes the access point. So NEMO is an extension of Mobile IP that would enable devices of these networks to maintain unchanged (in the sense of unchanged IP and network prefix) connections to other devices on the Internet.

The following definitions are important for understanding the basis of NEMO:

- Access Router (AR): Router that provides internet access to the Mobile Router.
- Care-of Address (CoA): IP address of the Mobile Router at its current attachment point.
- Correspondent Node (CN): An IPv6 device that is communicating with the Mobile Network Node via IP.
- Home Agent (HA): Host on the Home Network that enables the Mobile Router to roam.
- Home Network (HN): Network that a Mobile Router belongs to when it is no roaming. The network that is associated with the network link of the Home Agent.
- Home Address (HoA): The Mobile Router's address in the Home Network. It will be maintained when the MR roams to a foreign network.
- Mobile Network Node (MNN): Any IP device in a mobile network. It can be fixed to the mobile network or visiting the mobile network as mobile node. It does not need to be aware of the network's mobility.
- Mobile Router (MR): A router capable of changing its point of attachment to the Internet without disrupting higher layer connections of attached services.

Under NEMO, a MR takes over the role of the MN in performing mobility functions. Nodes that are attached to a MR, that is the MNNs, are not aware of the network mobility and do not perform any mobility functions. The MR sends binding updates to its HA communicating its new CoA. The HA will bind an entire network prefix to the MR's CoA and it will forward all the packets for that network to the MR. If a CN sends a packet to an MNN, the packet will be routed on the Internet to the corresponding HA, then this HA will tunnel the packet to the MR and the MR will deliver it to the MNN. Reverse packets take

the same path in the opposite direction, that is, the MNN sends packets to the MR to be tunneled to the HA and then sent to the CN via the Internet.

In the Figure 2 below the NEMO Communications Model is depicted

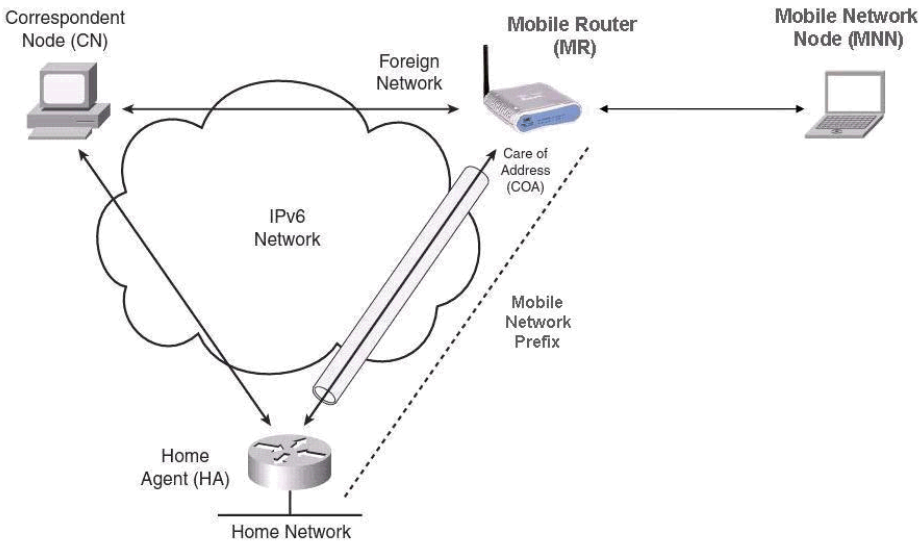

Figure 2 – NEMO Communication Model

The security issues in NEMO are higher than in MIPv6 because, in this case, a bigger number of nodes are involved. The recommendation is still to use IPSec in the communications between the MR and the HA. If any packet arrives at the MR outside the tunnel, they should be denied. And the MR should not send packets originating from the mobile network anywhere except through the tunnel to the HA. The MR should also perform antispoofing filtering to prevent spoofed packets.

2.6.3.Mobile Ad-Hoc networks

Mobile Ad-Hoc Networks (MANET) are networks that are formed dynamically by a group of Mobile Nodes. The topology is dynamic and arbitrary and is created "on the fly" as the devices move autonomously. MANET devices use wireless communication medium and very little bandwidth. IPv6 is well suited for MANET because each node would have a link-local address and a global address for the dynamic routing. Nodes use autoconfiguration to set up their addresses and form a network.

The routing protocols used in MANETs, such as Ad-Hoc On-demand Distance Vector (AODV) Routing or Optimized Link State Routing (OLSR) Protocol, are intended to be light weighted and do not have integrated security features. MANETs have several security characteristics:

- They cannot benefit from physical security.
- Due to the arbitrary association of nodes, it is difficult to perform authentication in an organized manner.
- Due to the little bandwidth and the desire to maintain nodes to be as simple as possible, encryption will probably not be widely deployed.

Therefore it would be relatively easy for an attacker to introduce bogus information or to cause a denial of service. These implications also lead to a higher risk of eavesdropping and snooping of packets.

Nevertheless, the signal power is low and the range is reduced, so the attacker would have to be geographically close to the MANET to be able to data over the air.

Little is known about the security of MANETs, but using shared keys or specific wireless link-layer encryption solutions could help to secure them.

2.7 Conclusions for IPv6 Secure communication

IPv6 is targeted to increase the available address space and to remove several limitations of IPv4. It allows autoconfiguration of node addresses and it performs more efficient features of Security and mobility over IP.

But whilst IPv6 changes the way you communicate, the security architectures must adopt to the changes. If IPv6 is deployed without taken into account security issues, it is like running a backdoor protocol to the dual-stack systems that could potentially be exploited.

In this section some best practices for securing the IPv6 infrastructure have been proposed, but it will be required a continuous learning process while IPv6 is being adopted.

3. Partial modules of Secricom solution in IPv6 environment

3.1. PTT Enhancements by IPv6

In the area of communication the LTE technology and IPv6 framework could be considered to be the state-of-the-art, however it is yet not widely spread. IPv6 offers many technological advantages as stated in other parts of this document and event the European Commission encourages the widespread adoption of its sixth version. It is no doubt the LTE will be the dominating standard of 4th generation mobile communication networks but the problem is - it is not widely used today.

Our main objective is integration with existing systems, not the creation of a new isolated communication island so we must take into account the current situation. The most common and important data bearer today – the GSM mobile network and 3G technology do not support IPv6 or more precisely the network operators do not support it over their network, not mentioning QoS.

As we are moving towards an information-driven society, increasingly relying on ICT tools, the development of a converged communication and service infrastructure that gradually will replace the current systems, mobile, fixed, and audiovisual networks is fundamental and not only in the domain of crises management.

LTE is the first true All-IP packet based mobile network enabling all kind of IP-applications with high data rate. Thanks to shorter TTIs (Transmission Time Intervals) also IP roundtrip time will significantly reduce. Life tests revealed roundtrip times smaller than 18 ms and practical data rates of 60 Mbit/s. This is a significant reduction compared to GSM circuit switched voice service which was specified to have less than 120 ms delay on a single direction. It can be observed that for high user acceptance not only average data download speed is important but also reaction time, especially in crises management situations. The reaction time (influenced by the network latency and jitter) is the biggest drawback of current mobile IP based communication systems when compared to traditional tactical radios. What's needed is a user experience of "click and wow". Also there is growing interest in real-time services, whereby VoIP just is the simplest of those. Triple Play applications combining voice+data+video are gaining momentum. Remote database access and data communication in a network of multiple users accessing a common application requires fast reaction. A good example for this application could be the added value when incident commander can use a single application not only to talk to his team but to watch real-time video feed from security camera installed in the exposed area or CCTV, look up information from other systems by using Smart Agents or manage resources etc.

3.1.1. Preparation for future

The Internet Protocol version 6 (IPv6), on the basis of a specific action plan, should be fully implemented by 2010. The leading mobile operators and manufacturers around the world have already committed to using the LTE standard as well. These new technologies will allow more enhanced services for users and should provide better means to control QoS.

The architecture of the first version of our communication platform will not be pure IPv6 solution utilizing all the benefits that the new enhanced IPv6 offers. The reason is the fact that the switch from IPv4 to IPv6 will not happen globally and overnight and there are still a lot of technologies and systems that will not be able to use it for some time. To fulfill our integration and communication seamlessness goals we have to support old proven technologies and the new ones where appropriate. Our answer to this challenge is a Dual-Stack. Both our communication servers and client application on all platforms, including mobile phones, PDAs, will use dual stack. If the network supports version 6 of the protocol our client application will prefer this one. Depending on the version of the protocol the client applications will provide more features to users, e.g. direct VoIP call between two mobile devices without the need to use a server and special NAT traversing protocols such as ICY or STUN. The direct call or multi cast group calls will be made easier when all the devices will have its own unique public IP address and the overall system resilience will be improved.

The most important benefits of IPv6 for our communication platform:

1. IPv6 provides a substantially larger IP address space than IPv4
2. IPv6 provides better end-to-end connectivity than IPv4
3. IPv6 has better ability for auto-configuring devices than IPv4
4. IPv6 contains simplified Header Structures leading to faster routing as compared to IPv4
5. IPv6 gives better Quality of Service (QoS) than IPv4
6. IPv6 provides better Multicast and Anycast abilities compared to IPv4
7. IPv6 offers better mobility features than IPv4
8. IPv6 offers ease of administration over IPv4
9. IPv6 follows the key design principles of IPv4, thereby permitting a smooth transition from IPv4.

Most of the benefits will be in the area of network management and QoS. Of course for backward compatibility purposes we are not able to use all the benefits in PTT at once. The first versions will use the server client approach (start topology) and later on we will try to move the architecture more and more towards distributed system.

3.1.2. Communication services and IPv6

In general our communication platform is not dependent on particular version of a protocol. The most important thing for the communication to work is to have the connectivity and the way it is provided is more related to infrastructure then the communication applications themselves.

Our solution is using two IP stacks, which one is used is decided during runtime and it depends on the configuration of the device and which link has connectivity enabled. Our servers are able to communicate with both types of client protocols at the same time. To simplify the client device configuration we have implemented support of DNS instead of direct IP address configuration. The DNS name of the primary server (more precisely server cluster) is part of the user name (in the form: user@server.eu). The DNS server then returns the IP address in the format suitable for the client, e.g. if the client application is requesting

the IP address using IPv6 the server returns IPv6 address of our communication server or IPv4 otherwise. To allow the compatibility and seamlessness of communication not only between IPv4 and IPv6 client application but between other communication systems as well we are using the star topology where all the communication is traveling to or from the sever and not directly between clients (some exceptions apply for direct IP calls).

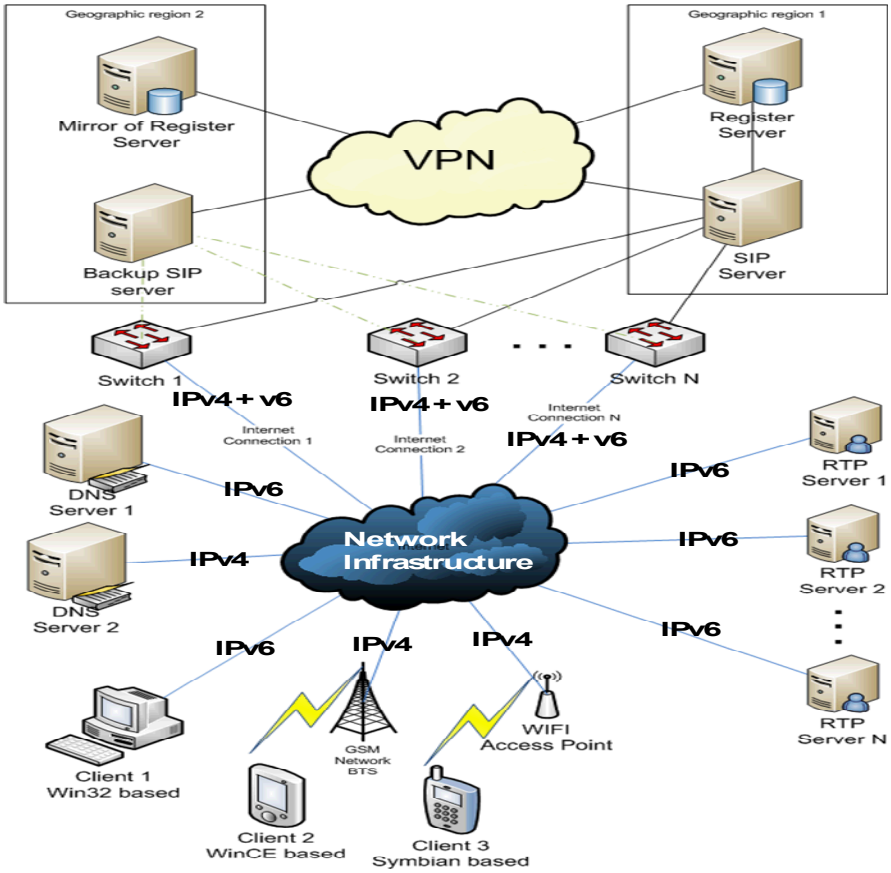

Figure 3 - Sample scheme of deployment and used protocol version

This approach allows us to keep strong end-2-end security avoiding possible Man-in-the-middle attacks even between different systems, there is no need for a tunneling or NAT-PTs or address pools. Furthermore the group addresses will allow us to use easier load balancing and high availability techniques.

3.1.3.The quality of service

The quality of the link dictates what level of service the application is able to provide to the user because the system must provide linear degradation instead of total denial of service when link quality degrades. The routers and especially the MBR will be able to apply the routing policies based on the bearers that are currently available and the type of traffic and its priority but first it needs to know what type of traffic it is. For this purpose we will use the header extensions offered by the IP protocol. It is also important not to forget that the end user application must be able to show this change in network quality to the user so that the user is not trying to transmit large file and wondering why it is still not transmitted when the infrastructure has hard time to service the higher priority communication such as voice.

Figure 4 – Sample screenshot from PDA

As mentioned earlier the IPv6 provides better means for QoS management and DoS protection. Our servers will be able to negotiate or at least query the level of service the infrastructure is able to provide for a particular client and it will inform the client application so that the user can clearly see what services he/she could use. For example if user A has 2Mbit/s connection to the server and user B has only 9kbit/s the server will not route video feeds from CCTV to user B, nor will allow user A to initiate a video call with user B.

Usually the worse connectivity links (bearers) do not support IPv6 but use IPv4. It is obvious that IPv6 has to use bigger headers and this increases the protocol overhead and might have a negative influence on the communication delay and thus on quality on low performance links.

3.1.4. The security

The improved security and IPSec features provided by IPv6 do not provide significant benefit for our communication platform. We have to consider the user requirements (related to user accountability). The system must provide user-2-user authentication and confidentiality and this means it has to be implemented on higher layers of protocol stack.

Layer	Example
Application	Our security framework is implemented here
Presentation	
Session	PTT Sessions, signaling, half/full-duplex conversations
Transport	TCP for signaling, UDP for voice, video
Network	IPv4/ IPv6/ IPSec
Data Link	
Physical	802.11a/b/g/n, 3G, LTE

Figure 5 – Implementation of additional security

The security mechanisms protecting just the communication channel between two network nodes are simply not enough. The fact is that applications and systems used by special incident response teams will be required to be compliant with standards such as FIPS, Common Criteria, and pass several security evaluations and certifications. Another important aspect is the fact that the IPv6's security attributes have not been verified by time and there are still several known threats. It is also recommended that the early adopters of IPv6 exhibit caution when it comes to security. It is part of our risk management strategy that we use our own security framework to protect the user.

Our solution is using standard and proven approaches build on PKI, user and server certificates, dedicated crypto hardware for key generation, exchange, and storage or encryption acceleration. Trusted Docking Station provides additional security and trust into the execution environment.

It is out of scope of this document to describe the security concept in detail but our approach and architecture is compliant with standards and certifiable up to NATO Confidential.

3.1.5.Secricom PTT architectural decisions related to IPv6

- Each PTT server will have both IPv4 and IPv6 addresses and we will use DNS name instead of exact IP (actually it will be a bit more complicated, the address in DNS will be a virtual address of failover/load-balanced server cluster). The question is how to connect servers within the cluster as these will need to be placed in geographically different places.

- User's PTT address will look like an e-mail address and the client application will ask DNS for PTT server's address by parsing the name after @(e.g. hudek@pttserver.secricom.eu). The DNS server should be configured in such a way that it will return IPv4 or IPv6 address based on the protocol that was used by the client to ask the DNS server.

- The client application will use special component (preliminary name: "Connectivity Wrapper") as an abstraction from protocol specifics so that more benefits of IPv6 could be used in the future should we decide to go pure IPv6.

- We have used a different port for each session until now. We plan to change it to use a different port for different type of stream's content and all the data of the same content type will use the same port number regardless of the session to which the data belong. This way all audio communication will be on port X, signaling on port Y, pictures on port Z etc. It will help to define routing and priority policies in the infrastructure.

- The PTT Gateways will need connectivity to PTT servers and another system they integrate to (we expect IPv4 mostly).

- Another issue is PTT server to PTT Server communication. The most of the communication traffic will be between users of one server but some users will need

to communicate with users of different PTT server in different/remote location (IPv4 probably).

The windows applications will prefer IPv6 if available, the other client applications will depend on device's and network's capabilities.

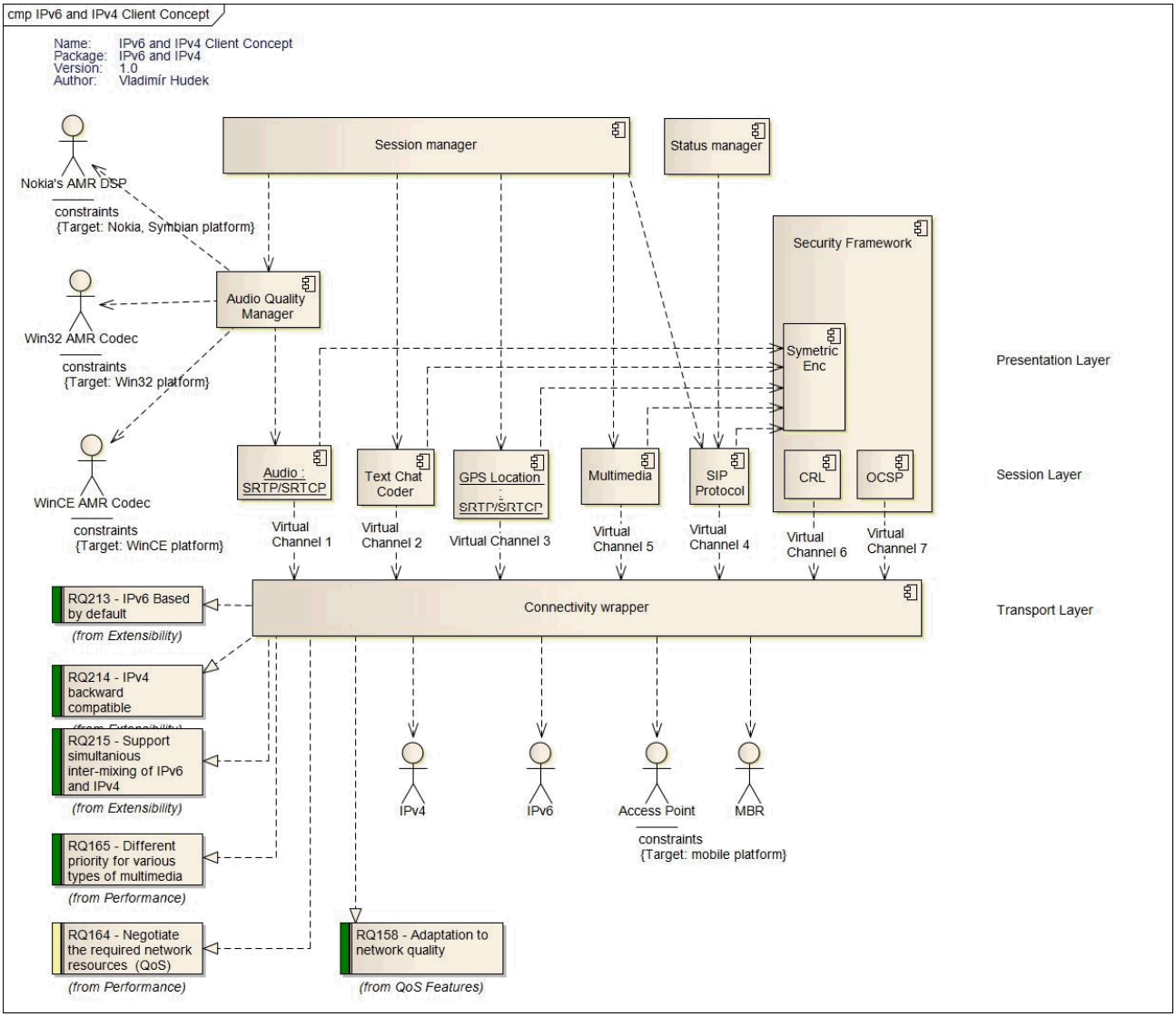

Figure 6 - Secricom IPv6 and IPv4 PTT Client Concept

3.1.6 Comparison between IPv4 and IPv6 overhead

# audio packets	RTP size [Bytes]	RTP size [bips]	Protocol Delay [ms]	Bitrate with UDP header [bips]	Bitrate with IPv4 header [bips]	Bitrate with IPv6 header [bips]
1	30	12000	20	15200	21600	24800
2	46	9200	40	10800	14000	15600
3	62	8267	60	9333	11467	12533
4	78	7800	80	8600	10200	11000
5	94	7520	100	8160	9440	10080
6	110	7333	120	7867	8933	9467
7	126	7200	140	7657	8571	9029
8	142	7100	160	7500	8300	8700
9	158	7022	180	7378	8089	8444
10	174	6960	200	7280	7920	8240
11	190	6909	220	7200	7782	8073
12	206	6867	240	7133	7667	7933
13	222	6831	260	7077	7569	7815
14	238	6800	280	7029	7486	7714
15	254	6773	300	6987	7413	7627
16	270	6750	320	6950	7350	7550
17	286	6729	340	6918	7294	7482
18	302	6711	360	6889	7244	7422
19	318	6695	380	6863	7200	7368
20	334	6680	400	6840	7160	7320
21	350	6667	420	6819	7124	7276
22	366	6655	440	6800	7091	7236
23	382	6643	460	6783	7061	7200
24	398	6633	480	6767	7033	7167
25	414	6624	500	6752	7008	7136
26	430	6615	520	6738	6985	7108
27	446	6607	540	6726	6963	7081
28	462	6600	560	6714	6943	7057
29	478	6593	580	6703	6924	7034
30	494	6587	600	6693	6907	7013
31	510	6581	620	6684	6890	6994

Table 2 - Comparison between IPv4 and IPv6 overhead

3.2. SDM Enhancements by IPv6

The Trusted Self-Organizing Relationship Network, which is provided as component by the Secure Docking Station, provides versatile trusted interactions (relationships) between different attestable entities on top of an existing reliable communication infrastructure, as provided by the Multi Bearer Router (MBR) in the SECRICOM architecture. In this context the term 'self-organizing network' represents the interaction of trusted entities in a virtual network which cannot be mapped to the real infrastructure of an underlying network. TSORN in combination with the SDM is responsible for attesting the state to any remote party in the same virtual network.

The TSORN component creates a trusted and secure overlay with other SECRICOM devices which are reachable over any IP capable infrastructure including multi-hop environments. TSORN therefore has built-in routing mechanisms which provide paths to every TSORN member as long as it can be addressed using IP.

3.2.1. Trusted Communication and IPv6

In general TSORN is not dependent on any particular version of the IP protocol. But since there are several issues, especially regarding network address translation (NAT) and security, in IPv4 which are currently not solved or unsatisfactory, the use of IPv6 will eliminate the need for complex and inconvenient workarounds.

Therefore, in case of TSORN it will very beneficial to use IPv6 as underlying protocol especially because TSORN does not reference IP addresses internally but rather node IDs. All internal communication and addressing is handled using these IDs. IDs of other nodes are usually learned through the network itself. Because each peer keeps track of the network member list which is synchronized globally through gossip, thus all peers know from each other eventually. If a particular node, with whom a trusted communication process should be started, is not a local neighbor than a route discovery process is started. The route discovery process tries to find a path to that specific member node using its neighbors. Each neighbor node itself checks if it has a route available and returns it otherwise the same process as before is started until the destination is reached and the route is returned or a discovery timeout has occurred.

Thus, neighborhood detection and management is of paramount importance in TSORN. There are 3 different mechanisms to discover neighbors.

- Broadcasting a neighbor request message to the network and using the responding nodes for the neighborhood. Sending a multicast message to a multicast address falls also in this category.
- Try to use other nodes from the member list as neighbors intelligently in order to reduce route lengths.
- Provide IP-ID mappings to TSORN which are then used to discover these nodes and add them if available.

We have 2 interaction points with IP addresses, the IP-ID mapping and the multicast address. But since these addresses are solely used to open a socket to that node it doesn't

matter if it is an IPv4 or IPv6 address. Thus, TSORN is perfectly IPv6 capable without modifications and also gains much simplicity from the broader address range and the eliminated need for NAT and subnets.

3.3.IPv4/6 Support on the Multi-Bearer Router

3.3.1 Introduction: SECRICOM User Requirements

As a communication system for crisis level emergency, SECRICOM user requirements call for a need to provide for:

- Business continuity across different agencies and across European members states;
- Business continuity across the strategic, tactical and operation spaces and seamless inter-connected fashion;
- Business continuity in a disaster zone, where previously installed fixed infrastructure may be destroyed or severely degraded and hence cannot be relied upon to provide adequate communication services;
- Security in terms of confidentiality, integrity and availability;
- Simplicity and flexibility to achieve ease of deployment.

3.3.2 Mobile Ad-Hoc Networks

The term ad hoc networks is used to denote networks which are created 'on-the-fly' (ad hoc) and sometimes on an as-needed basis. Because of its implication to user mobility, the term is often associated with networks that use a wireless medium for its communication. Whilst, the term ad-hoc networks almost always means ad-hoc wireless networks, ad-hoc wired networks is still possible e.g. where multiple portals of varying service provisioning and costs are concerned.

In contrast, the term Mobile Ad-Hoc NET works (MANETs) refers to ad-hoc networks in which the communication nodes forming the ad-hoc network are mobile. Such networks are often formed on an as-needed basis and do not generally require the existence of a fixed infrastructure. This property makes ad-hoc wireless networks suitable for use in various scenarios like crisis/disaster-level incidents, battlefields or in areas where user density is too sparse or too rare to justify the deployment of network infrastructure economically. Figure 7a and b below shows some examples of ad-hoc wireless networks.

3.3.2.1 Coverage of Ad-Hoc Networks

Ad hoc networks may be classified on the basis of their geographical coverage capability, and generally fall into three categories, namely:

- Ad-hoc personal area network (PAN),
- Ad-hoc local area network (LAN), and

- Ad-hoc wide area network (WAN).

3.3.2.2 Routing in Ad-Hoc Networks

In fixed wired/wireless networks, dedicated routing devices are often used to achieve the process of packet routing. Because of the static nature of these networks, where network topology almost never changes, it is relatively easy to proactively distribute the topology of the network amongst the routing devices, thus enabling each router to pre-compute and maintain routes to other routers.

In contrast, mobile ad hoc networks do not have a fixed routing infrastructure in principle and hence suffer from the inherent limitation that the network topology may change rapidly and unpredictably as nodes move. In the absence of fixed routing infrastructure, the nodes forming the ad-hoc networks themselves have to act as routers. A MANET may therefore be defined as an autonomous system of mobile routers (and associated hosts) connected by wireless links.

Given the central importance of routing in ad-hoc networks, it is not surprising that routing forms a basis for classifying ad hoc networks into two groups, namely:

- Single-hop ad hoc networks, see **7**a, where nodes do not act as routers and therefore communication is possible only between nodes which are within each other's wireless range, or via a fixed infrastructure and
- Multi-hop ad-hoc networks see 7b, where nodes are willing to act as routers and route or forward the traffic of other nodes.

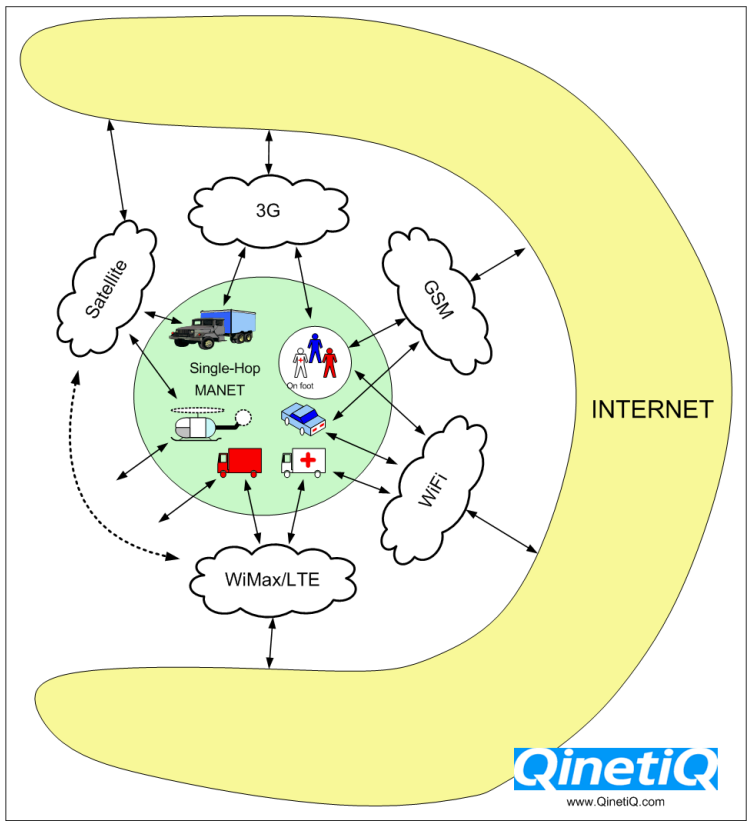

Figure 7a – Single Hop

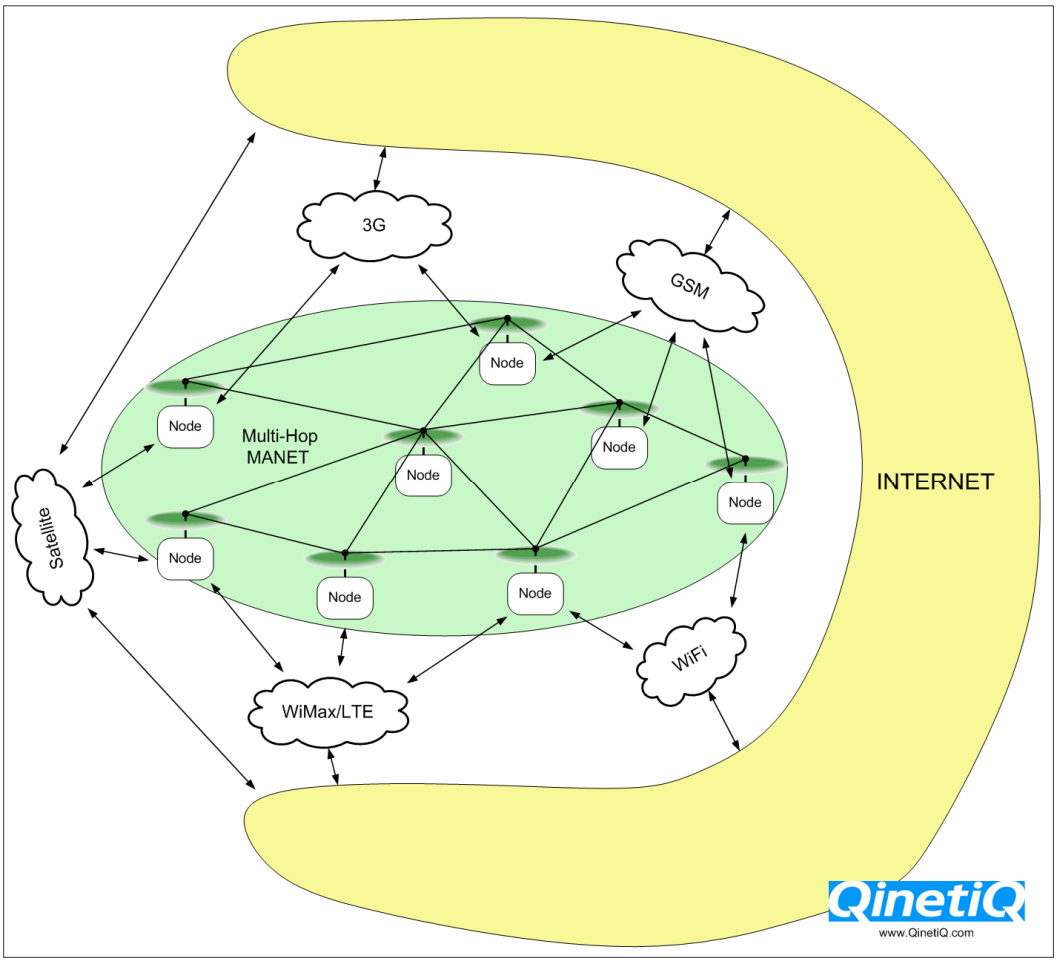

Figure 7b – Multi-Hop (Types of MANETs)

3.3.3 IPv4 and IPv6

Internet Protocol version 4 (IPv4) enables network connectivity in a wide variety of government and commercial systems worldwide, including the Internet. Version 6 of the protocol (IPv6) offers a number of potential benefits over IPv4. These include a massively increased address space, more efficient processing in routing infrastructure, automatic configuration of end hosts and built-in support for Quality of Service (QoS), Mobility and IP Security (IPsec). IPv6 implementations are being offered in a number of network products and for some systems a gradual migration to IPv6 has being on going. The pace of transition is highly variable, depending on the attractiveness to system owners of the IPv6 features. For example, western nations tend to have sufficient IPv4 address allocations and are less urgently motivated towards IPv6 than nations in the Far East.

3.3.4 MANETs and IP support for SECRICOM Requirements

By their nature, IP MANETs offer the opportunity to fulfill some of SECRICOM requirements, some of which are given below:

- Deployable networks to support extended business continuity within a greater disaster geography, where previously installed fixed infrastructure may have been destroyed or severely degraded;
- Seamless inter-connectivity amongst fixed, nomadic and mobile nodes within which strategic, tactical and operation users are dispersed;

- IP ubiquity leading to a great support for interoperability across different agencies belonging to different EU states;
- Improved users within the operation space mobility furnished by greater support for mobility by IPv6;
- Increased ease of deployment; and network performance and management through QoS and/or stateless auto-configuration leading to better improved network operability;
- Mandatory support for security in IPv6 plus extension headers could support optional security extensions leading to a general improved network and information security;
- Greater scalability and simplicity in addressing and routing, plus flexibility to meet future requirements leading to simplicity and flexibility.

Besides usage of legacy/existing networks, SECRICOM should also be able to make use of a dedicated emergency fast-deployed network as part of the response procedure of the emergency services. Thus, it may be said that SECRICOM is expected to provide business continuity over both IPv4 and IPv6 networks and that there is a requirement for the Multi-Bearer Router (MBR) to operate over and provide support to SECRICOMs applications within

- Pure IPv4 networks,
- Pure IPv6 networks,
- Mixed IPv4/IPv6 networks, and
- Mixture of IPv4/IPv6 applications.

Consequently, the following four assumptions are made:

- 'Native SECRICOM networks' are IPv6 in principle, but with the potential for IPv4 end applications, e.g. legacy, being deployed within those native SECRICOM networks,
- SECRICOM requires the ability to exchange traffic with both IPv4 and IPv6 non-SECRICOM end hosts,
- SECRICOM requires the ability to exchange traffic over both IPv4 and IPv6 non-SECRICOM networks, and
- The SECRICOM network management is in principle IPv6, but may be required to manage IPv4 end hosts.

Alternatively stated, there is a need for the MBR to interoperate with both IPv4 and IPv6 networks.

3.3.5 Routing Architecture

In order to support interoperability over IPv4 and IPv6 networks, simultaneous IPv4 and IPv6 support is necessary on any SECRICOM routing device, including the MBR. There are two techniques for achieving this interoperability

- Dual stack at the edge, and
- IPv4-over-IPv6 and IPv6-over-IPv4 tunnelling over the single/multi-hop MANETs and subsequent bearer networks.

Figure 8 gives the routing architecture achieved by the MBR. Here, a native SECRICOM end network is assumed to contain IPv6 end devices by default but may also contain IPv4 end devices as well in order to cater for legacy equipment.

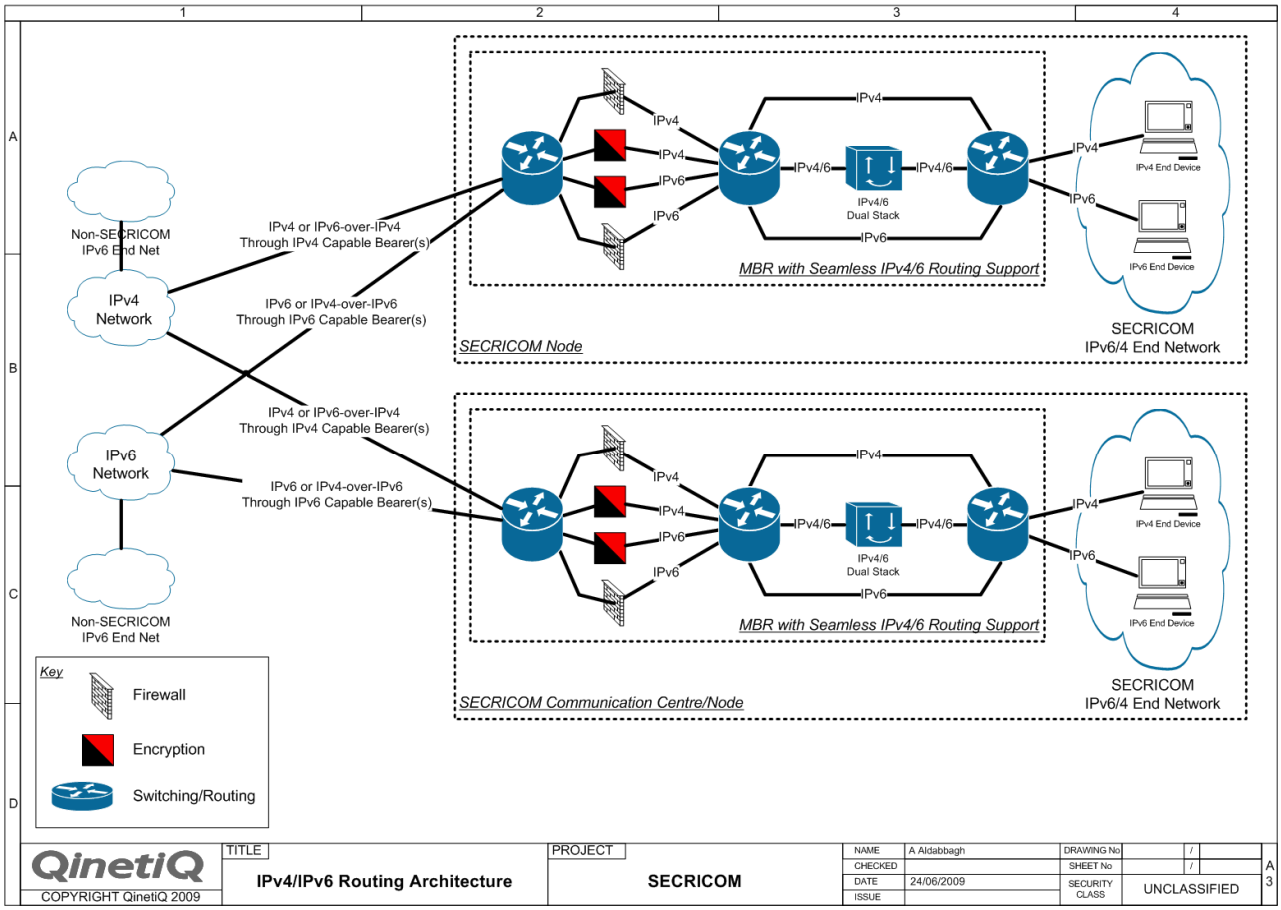

Figure 8 – MBR Routing Architecture Achieving IPv4/IPv6 Interoperability

The routing architecture takes into consideration the following aspects:

- Seamless IPv4/v6 routing, thus allowing legacy applications to continue to operate in a seamless manner, and
- Aspects of resilience, e.g. passage of IPv4 traffic over IPv6 networks and vice-versa.

The current strategy is to turn the MBR into a platform for supporting seamless IPv4/6 routing. That is, from a routing perspective, the end devices should be able to communicate across any bearer network(s) regardless whether the bearer network is IPv4 or IPv6.

To this end, adds flexibility by allowing:

- An end device IPv4 traffic to be forwarded by the MBR without any conversion,
- An end device IPv4 traffic to be 'converted' to an IPv6 via the use of a dual stack prior to being forwarded by the MBR,
- An end device IPv6 traffic to be forwarded by the MBR without any conversion,
- An end device IPv6 traffic to be 'converted' to an IPv4 via the use of a dual stack prior to being forwarded by the MBR,

IPv6 can be tunneled over IPv4 networks and vice versa thus increasing resilience on the carrier network side.

3.3.6 MBR Development

QinetiQ has undertaken the task of implementing the architecture given in **Figure 8** onto the MBR. At the time of producing this document, QinetiQ has completed the software coding phase of the implementation and is about to start the testing phase.

3.3.7 Concluding Remarks

This section has briefly described a subset of the SECRICOM user requirements that have impact onto the SECRICOM network/communication design. IP MANETs has been shown to provide the basis for reliable inter-connectivity to support business continuity across the fixed, nomadic and mobile nodes within which strategic, tactical and operation users are dispersed and across different agencies belonging to different EU states. A routing architecture was described which could achieve IPv4/IPv6 interoperability in a seamless manner.

3.4.Monitoring Solution for Secricom

The solution for monitoring proposed in Secricom project will be mentioned and also its current IP version compliance will be described. But before presenting this solution, some considerations should be taken into account in the solution infrastructure design.

3.4.1.Design Considerations

Due to the bandwidth constraint that most mobile networks have, some aspects related to policy based network management should be implemented. Depending on traffic load and link availability, router decisions will be made.

Another common issue of mobile networks probably will be the constraint of intermittent communication links. This problem should be mitigated by supporting off-line performance in the agents.

In order to achieve a good snapshot of the security state of the Secricom network, the agent infrastructure should be deployed in a distributed manner. So agents will collect information from the network and will send it to the server when both link connectivity and the server are available. The rest of the time, the agent will be a stand-alone infrastructure that will report the collected data when the link will be available again.

It is also worth to consider the possibility of deploying a secure environment for agents-network sensors. This could be achieved by sitting the agents alongside the Multi Bearer Routers (MBRs), which could likely result not efficient due to the requirements. Another option would be to have the agent embedded within the MBR.

The final objective is to achieve a level of trust between the agents and the server, in terms of network management. This idea could be similar to the model used by SDM and TDS, but in the network management level.

3.4.2.Monitoring Solution Description

In the following picture the monitoring infrastructure for Secricom is depicted.

As it is shown on Figure 9, the solution is mainly based in four elements, the server, the agents, the database and the framework.

- The server is responsible for performing the processing tasks. It will be in charge of collecting data from agents, priorizating the received security events, defining the security policies, defining the correlation rules and linking the different integrated tools.
- The agents are the responsible of collecting data from the network and send it to the server in a standard format, for making the processing and the storing easier.
- The database is the place where all the detected events will be stored, for its later processing.

- Finally the framework is the responsible of managing all the modules.

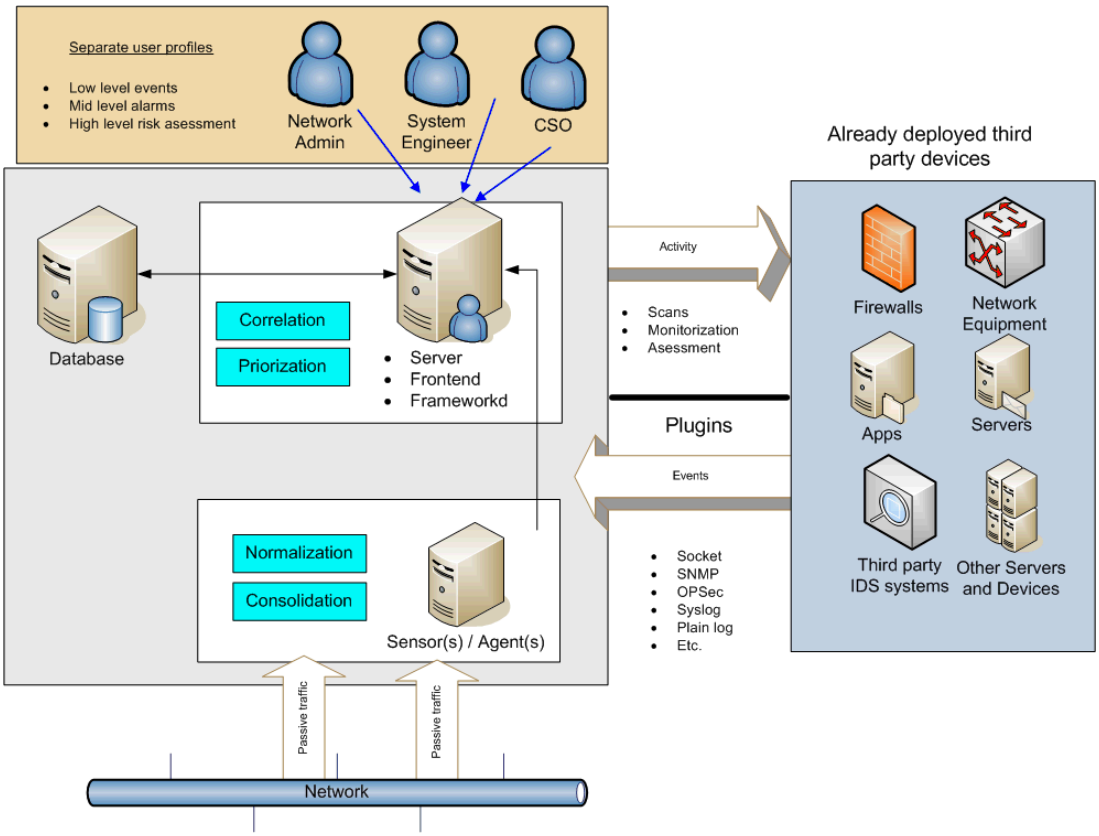

Figure 9 - Secricom Monitoring Infrastructure

3.4.3.Integrating into SECRICOM solution

It would be necessary to monitor some of the features of the MBR related to its performance. In the next Figure 10, is shown how the solution could be integrated into Secricom solution.

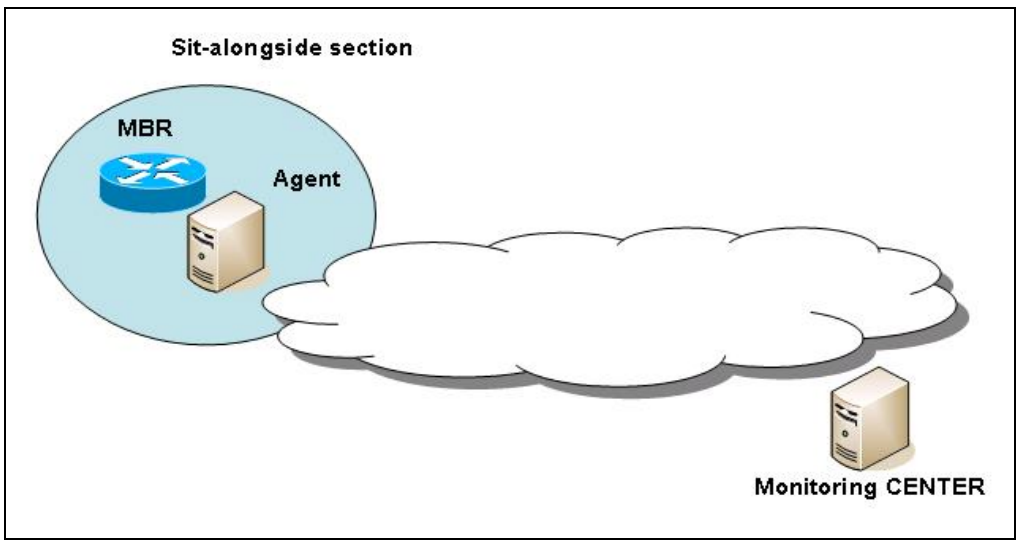

Figure 10 - Secricom Monitoring Infrastructure integration

On one hand, it could be possible to distinguish the location of the agent maybe as a sit-along-side possibility; the agent will be placed next to the monitoring target system, i.e. the MBR, or maybe embedded in the MBR, where this would be solved in the network design. This could be a distributed architecture of agents. In this way, security information will be collected by the agent and stored and after processing, it will be sent to the Monitoring Center.

On the other hand, there is the Monitoring Centre, where all the events detected by the agent in the monitored system will be collected and processed in a remote way, to determine the security status of these systems. Monitoring centre is currently able to detect events and alerts using the information provided by the agents.

In order to reduce traffic load on the network, it would be desirable to reduced the information sent and correlate the collected information by the agent itself, and sending only an information summary with the most relevant events.

It would be desirable to work in online/offline mode, so that when the link between the agent and the server is not available, the agent will be able to work in a standalone mode and send the information collected during the silence period when the link is available again.

3.4.4.Monitoring Components

In terms of monitoring there are some capable tools which provide useful information in different subjects

- Network monitoring.
- Bandwidth management
- Other types of agents deployed in remote network/servers and reporting to a central server
- Data detection in terms of IDS, but higher requirements are necessary to establish an interface to listen in the network in promiscuous mode.

In the following list, there are the some of the most important tools that are integrated in the monitoring solution:

- Snort: traffic sniffer and network intrusion detector, it includes an attack detection engine and a port sweep that allows it to store, to alert and to respond to any previously defined anomaly.
- Nessus: vulnerability scanning program over several operating systems. It starts with a port scanning looking for open ports, and then it tries some attacks over them.
- Openvas: Nowadays Nessus is not a free tool anymore, so it could be an alternative replace it by Openvas, which stands for Open Vulnerability Assessment System and is a network security scanner.

- Ntop: real time monitor of the users and applications that are consuming network resources in a specific moment and it is able to aid in the detection of system and service misconfiguration.
- Nmap: TCP and UDP port tracker, it is used to assess the computing system security and to discover services and servers in a computing network.
- P0f: tools for passive identification of the operating system, it allows to detect the network computers system and version.
- Nagios: system for monitoring the specified systems and services, alerting when the behaviour of the network is not appropriate and when it becomes satisfactory again.
- Arpwatch: ARP (Address resolution Protocol) activity monitor, its main utility is the ARP spoofing detection.
- NDPMon: ARP is for IPv4 as NDP (Neighbour Discovery Protocol) is for IPV6, so the equivalent tool of Arpwatch for IPv6 will be NDPMon (IPv6 Neighbour Discovery Protocol Monitor). NDPMon observes the local network to see if nodes using neighbour discovery messages behave properly. When it detects a suspicious Neighbour Discovery message, it notifies the administrator by writing in the syslog and in some cases by sending an email report.
- Pads: firm detection engine, used for the passive detecting of the network assets. It is designed for complementing the IDS technology, providing a context to the alerts.
- Snare: it is a tool that facilitates the real time transfer of the Windows event log information.
- Osiris: system integrity monitor that periodically monitors the systems looking for changes.
- Ossec: host intrusion detection that performs register analysis, integrity checking, rootkit detection, time sequence based alerts and active response.
- OCS Inventory: it is a tool that collects hardware and software information for the surrounding systems.
- GLPI: it is a program for the management of a computing resources park.
- Tcptrack: It is a sniffer which displays information about TCP connections it sees on a network interface. It passively watches for connections on the network interface, keeps track of their state and displays a list of connections. It displays source and destination addresses and ports, connection state, idle time, and bandwidth usage.

3.4.5.IPv4-IPv6 compliance

In the following table, the compliance with IPv4 and IPv6 of the tools that should be included in the monitoring solution and that have been described before is shown.

Tool name	Current version	
	IPv4 Support	IPv6 Support
Snort	Snort-2.8.5	
	✓	✓
Nessus	Nessus-4.0 / Nessus 3.2.1 last free version	
	✓	✓
Openvas	Openvas-client-2.0.5 Openvas-server-2.0.3	
	✓	✖
Ntop	Ntop-3.3.10	
	✓	✓
Nmap	Nmap-5.00	
	✓	✓ (limited to some features, Nmap-2.54BETA6 version supports IPv6)
P0f	P0f-2.0.8	
	✓	✖
Nagios	Nagios-3.2.0	
	✓	✓
Arpwatch	Arpwatch-2.1a15	
	✓	✖
NDPMon	Ndpmon-1.4.0	
	✖	✓
Pads	Pads-1.2	
	✓	✖
Snare	Snare-setup-3.1.6	
	✓	✖
Osiris	Osiris-4.2.3	
	✓	✖
Ossec	Ossec-2.2	
	✓	✖
OCS Inventory	OCSNG-unix-server-1.02.1	
	✓	✓ (with an extra package)
GLPI	Glpi-0.72.21	
	✓	✖
TcpTrack	Tcptrack-1.3.0	
	✓	✖

Table 3 - The compliance with IPv4 and IPv6

3.4.6. Another possible monitoring tools

Related with bandwidth management, the software described below could be used in terms of coexistence between IPv4-IP6.

- **MRTG: Multi Router Traffic Grapher**

MRTG can monitor network consumption both over IPv4 and over IPv6. This tool can gather IPv4 or IPv6 router interface traffic volume statistics and it can show histograms of historical network throughput and other important metrics. Thanks to the graphs shown by the tool, it makes it easier for the network administrator to distinguish anomalies that could indicate a security problem. With MRTG, it is possible to gain a quick view of the typical IPv6 traffic volumes and directions and to easily notice things that are out of the ordinary.

MRTG can be set up over Windows and Linux platforms. The current version is the MRTG 2.16.2 and it already supports IPv6.

- **NetFlow:**

NetFlow is a very useful tool for network performance monitoring. NetFlow technology provides, among other features, the functionality for network traffic accounting, usage-based network billing, network planning and DoS monitoring. NetFlow gathers information about the flows passing through the network devices. It collects data about the individual flows and sends them to a collector, where they will be analysed. NetFlow can also be used to look at traffic anomalies.

The current version is NetFlow version 9, and it supports IPv6. NetFlow version 9 can gather statistics on IPv6 traffic. However, it still uses IPv4 to export the flow records from the network device to the collector.

Once NetFlow is configured on the network devices, it is time to analyze the flows sent to the collector. There are several applications that can collect the NetFlow flows and derive meaningful information from the data. One of these tools is the real time monitor *Ntop*, which shows the protocol distribution, the amount of IPv6 traffic on the network and the different IPv6 host communications taking place in the network.

4. Quality of service

4.1.Background

In the late 60's, when the Internet era began, the network was small and simple – connecting mostly academic and research institutions, carrying traditional data, where all packets were of equal importance. There was no need to assign priorities for traffic – no real-time services, no need for a policy better than the "Best effort" one. There was no difference whether a packet was delivered in 5ms or 500ms; the most important thing was to deliver it unchanged. A few years ago an enterprise would have different networks for different services – like a private TDM-based voice network, ISDN for videoconferences, a multiprotocol LAN and IP network to the Internet. Nowadays, there is a growing trend to integrate all networks into one network (mostly IP-based network; since applications have migrated towards being IP-based) because of economic and technological advantages. In an ideal situation, a network will have almost unlimited bandwidth and packet delivery time infinitely close to zero , and so no packet delay variation will occur. But in real situations, with limited resources that very often result not sufficient, various applications may require various network conditions to work properly. Since many different services are transported through one physical medium, the "Best effort" policy becomes not sufficient any more, which brings about the need to implement Quality of Service (QoS).

Quality of Service is a broad term used to describe the overall impression a client will receive over a network. In short, this is achieved by prioritizing the network traffic in order to ensure that the most important data reach the target in the manner they prefer.

QoS does not improve the network performance at all; it just assigns resources efficiently in order to increase user satisfaction.

4.1.1.Transmission characteristics

To better understand the QoS policy, we shall begin with explaining basic traffic parameters:

- throughput,
- packet delay, latency,
- packet loss,
- packet delay variation (PDV), jitter,
- error rate.

Throughput is the average rate of successful message delivery over a communication channel, usually measured in bits per second or data packets per second. The Shannon-Hartley theorem states that the upper bound of channel capacity is:

$$C = B \log_2 \left(1 + \frac{S}{N}\right),$$

where:

C – capacity of the channel [bps]

B – bandwidth of the channel [Hz]

S – total received signal power over the bandwidth [W]

N – total noise over the bandwidth [W].

Throughput may be subdivided into :

- available throughput,
- guaranteed throughput.

Available throughput – as oversubscription is a common practise in many network operators, the throughput a user subscribes may not always be available. This often happens in home users access networks; the contracted service is described as "up to *some* Mbps", which means that users may achieve that bandwidth under light loaded conditions, but may be not able to achieve it consistently. This is most noticeable during peak times, such as early evenings. Certainly users may never exceed the contracted bandwidth.

Guaranteed throughput is the minimum data rate available for the customer for all of the time. Available throughput maybe higher, but shall not fall below the guaranteed throughput. Some networks operators offer services, usually more expensive, with assured in SLA data rate.

Throughput is often perceived as the most important part of the QoS policy. In most cases, the increase in throughput solves Quality of Services.

Packet delay or packet latency is the time needed for a packet to travel from source to destination. Despite marketing hype, packet delay may be extremely small but will never reach zero. Most traditional data applications are not vulnerable to delay, but VoIP or video chat may seriously suffer from big delay. Very big delay may also break the connection. Packet delay consists of:

- **Packetization delay** is the time needed to prepare packets for sending, i.e. for:
  - Creating packets – time needed to create a header. This time is negligible compared to the time it takes to populate the data portion.
  - Hydrating packets – time needed to fill the packets with data. Packing a large amount of data into a single packet may increase the overall network performance but on the other hand will increase the delay of a single packet. Sending a lot of small packets may increase the habit of real-time application but may saturate the network and CPU resources. In general, smaller packets inefficiently use CPU and bandwidth but with the larger ones it takes more time to fill them with data and they are more susceptible to poor network conditions. Choosing the optimal packet size may lead to significant improvements.

  Optimal packet size depends on application type and network conditions. In SECRICOM scenario it may be worth considering testing in order to find optimal packet sizes for different networks.

- **Serialization delay** – time needed to transmit a packet at a given output rate (to move from NIC transmit buffer into the transmission medium).

Serialization Delay[s] = Size of Packet[bit] / Transmission Rate[bit/s]

The Table 4 below presents the serialization delays for various link rates and packet sizes are shown.

Packet size	Link rate				
	64 kbit/s	1 Mbit/s	10 Mbit/s	100 Mbit/s	1 Gbit/s
64 bytes	8 ms	0,512 ms	51,2 µs	5,12 µs	0,512 µs
512 bytes	64 ms	4,096 ms	409,6 µs	40,96 µs	4,096 µs
1500 bytes	187,5 ms	12 ms	1,2 ms	120 µs	12 µs
9000 bytes	1125 ms	72 ms	7,2 ms	720 µs	72 µs

Table 4 - Serialization delays for various link rates and packet sizes

- **Fragmentation delay** – if a packet is larger than Maximum Transmit Unit (MTU), it needs to be fragmented into smaller packets, which results in extra delay and CPU saturation. Since fragmentation does not exist in IPv6 (packet size must not exceed the smallest MTU of a path), this delay type refers to IPv4 only.
- **Propagation delay** – time needed to travel from the sender to the receiver through transmission media.

Propagation delay = distance / wave propagation speed

Wave propagation speed is limited by the speed of light but for wireless communication it may be very close to it. For copper wires, it is usually between 67% and 75% of the speed of light. Packets speeds over most common interfaces are shown below:

- Thick Coax – 231,000 km/s.
- Fibre – 198,000 km/s.
- AUI Cable – 195,000 km/s.
- Thin Coax – 195,000 km/s.

– Twisted Pair – 177,000 km/s.

Switching delay – time spent in internetworking devices (bridges, switches and routers). This value depends on the switching architecture of devices, internal circuitry and CPU.

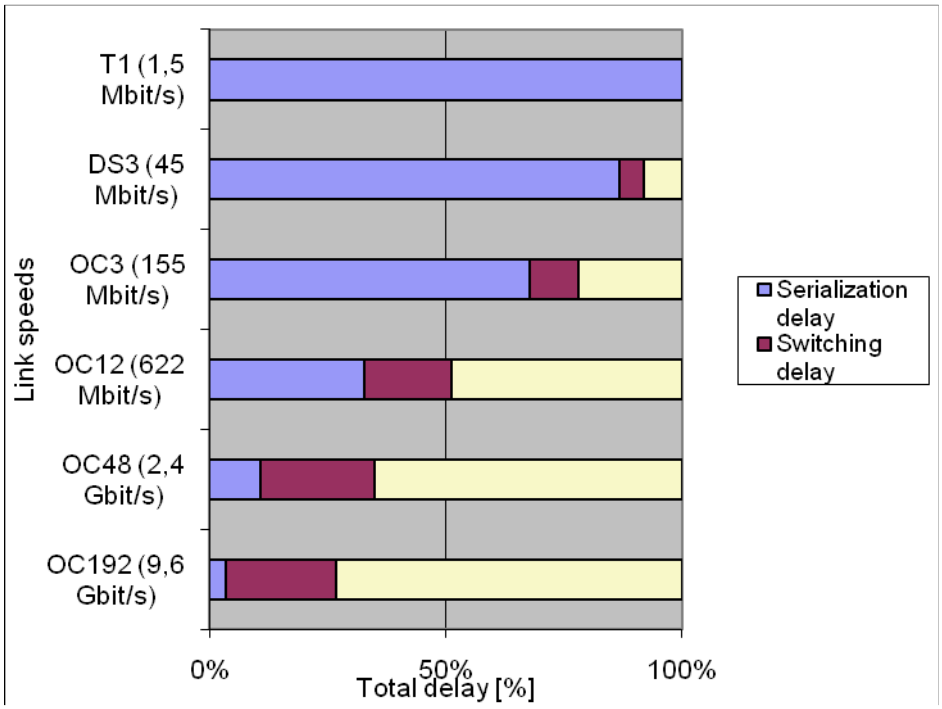

Figure 11 - Serialization delay and switching delay dependence

Packet loss occurs when a sent packet fails to reach destination. This situation may be caused by several factors, from signal degradation or faulty network hardware to routing routines. For most landline connections, the packet loss, measured in Bit Error Rate (BER), is very low, but in wireless networks it may make an application work incorrectly. As the wireless medium is vulnerable to environment and geographical conditions, like rain, landscape obstacles, interferences and high noise caused by sharing medium with different networks and technologies, packets may be lost in transmission. Wireless technologies often transmit redundant information since packets get dropped due to the nature of the transmission medium.

Redundant information has a significant impact on network performance. In case of poor medium conditions, it gives the possibility of recovering the damaged packet. But, on the other hand, it needs extra data to be sent, which saturates bandwidth. Choosing the optimal amount of redundant information should improve the network transmission.

Loss can also occur during network congestion. Packets that exceed queue limits may are dropped; this behaviour is a usual routing routine. Some protocols, like TCP retransmit dropped or corrupted packets. Retransmission saturates the network, which may result in more dropped packets, so the network becomes increasingly congested.

Because congestion has a significant impact on network performance, avoidances mechanisms are introduced in Congestion management.

Packet delay variation (PDV), also referred to as "jitter", is the difference between one way packet delay in a flow. The metric for the variation in delay of a packet is described in RFC 3393, where measurements between two hosts with or without clocks synchronized are proposed.

In traditional data transfers (like FTP, SMTP) PDV causes traced disturbances but for streaming protocols it may be a serious problem. By using a play-out buffer at the receiver side, the PDV problem may be mitigated (the media would just start a bit later), but for a real-time application, like VoIP or online games, PDV is a serious issue.

As mentioned above, the variation in packet delay is sometimes called "jitter". This term, however, causes confusion because it is used in different ways by different groups of people. Jitter commonly has two meanings: the first meaning is the variation of a signal with respect to some clock signal, where the arrival time of the signal is expected to coincide with the arrival of the clock signal. This meaning is used with reference to synchronous signals and might be used to measure the quality of circuit emulation, for example. There is also a metric called "wander" used in this context. The second meaning has to do with the variation of a metric (e.g. delay), with respect to some reference metric (e.g. average delay or minimum delay). This meaning is frequently used by computer scientists and frequently (but not always) refers to variation in delay.

Error rate is the measurement of the effectiveness of transmission. Error rate is the ratio of erroneous units of data to the total number of transmitted data. Like in a packet loss situation, when receivers detect a damaged packet, they should request the sender to retransmit it.

4.2. QoS policies

Network traffic is assembled of various flow types, generated by diverse applications that may need different performance. Network's capability to deliver services with some level of control over performance measures like bandwidth, delay, PDV and loss, is categorized into three service levels:

- Best effort (BE).
- Integrated services (Intserv, IS).
- Differentiated services (Diffserv, DS).

4.2.1. Best effort

Best effort may not be considered as a part of QoS, because it is just basic connectivity with absolutely no guarantee as to when or whether a packet would be delivered to the target. It is worth noticing that a packet will only be dropped if the routers' buffer queues are exhausted.

Best effort the only service supported by today's Internet. Most protocols, like SMTP, HTTP, FTP, IMAP work correctly with this policy, but some, e.g. VoIP, may suffer from high PDV and delay.

4.2.2.Integrated services

The Internet Engineering Task Force (IETF) in 1994 established a workgroup in order to build a model which would suit the needs of outgoing real-time audio-video applications. This task was divided into two subtasks – to construct a mechanism allowing an application to request for a resources, and routers to guarantee it.

The IntServ architecture was proposed in RFC1633, posted in 1994. The authors noticed that real-time applications often do not work well across the Internet because of PDV and losses. They also stated that there is a must for the Internet infrastructure to support real-time QoS, which provides some control over end-to-end packets delays before real-time application could be broadly used[1]. Another reason to introduce IntServ came from network operators, who were requesting the ability to assign the bandwidth on a particular link to different traffic classes.

Every supporting IntServ node must have implemented at least:

- Admission Control – checks if sufficient resources are available. If not, it refuses to set a connection.
- Traffic Classification – distinguishes traffic flows.
- Traffic Policing – checks that a flow does not exceed contracted parameters. If it does, packets may be dropped.
- Scheduling mechanism – arranges packet in queues.
- Signaling mechanism – spreads information about traffic classes around the network. RSVP is typically used as the signalling protocol, but IntServ is able to cooperate with different signalling protocols.

As every flow is treated separately, and studies have shown that an average connection is set for a short period of time, IntServ leads to network devices saturation. On top of that, network devices must be more complex to support techniques required by IntServ.

Integrated Services defines two classes of service:

- Guaranteed to service – described in RFC2212, provides deterministic delays. Guaranteed service is also named as *hard QoS*.
- Controlled load – described in RFC 2211, provides services closer to Best Effort policy.

Some authors consider Best Effort as a third kind of Integrated Services.

Resource Reservation Protocol (RSVP)

RSVP is a QoS signalling protocol for the Intserv architecture, providing the end application with the ability to signal their per-flow needs for network resources and routers to reserve it, but it is not a routing protocol and has no impact on which path will be chosen. RSVP was designed for multicast transmission, but it also supports unicast. The reservation is made one-way only, and for each path the sender, receiver and intermediate nodes may be shown.

[1] http://www.faqs.org/rfcs/rfc1633.html

RSVP uses *session* term to describe a flow of particular transport layer protocol to particular *session address*. The session address is defined by the destination node address and port number, and transport layer protocol ID. Every supporting RSVP node must be able to distinguish each session from packet flows. The session address may be either unicast or multicast. On top of that, RSVP protocol has capability to distinguish packets on the base of sending the node and protocol type. This feature may be used to privilege sending nodes (a packet from them would have reservation by default).

There are two ways of reservation defined in RSVP:

- **Distinct Reservation** – the flow originates from exactly one sender.
- **Shared Reservation** – the flow originates from one or more senders:
  - **Shared Explicit Reservation** – the senders list is explicit.
  - **Wildcard-Filter Reservation** – there are no explicit senders. All packets sent to a specified address will have reserved characteristics. But the reserved network parameters do not depend on the number of senders.

The RSVP also carries:

- Traffic Specification (TSpec) parameter – information about traffic characteristic.
- Resource Specification (RSpec) parameter – a set of needed network parameters.

This protocol was first mentioned in RFC 1633 in June 1994 and later defined in RFC2205 in September 1997. It is mostly used with real-time application, like audio or video streaming, although it may be used with any kind of traffic.

4.2.3.Differentiated Service

Differentiated Service (also referred as DiffServ or DS) is a scalable mechanism to provide Quality of Service. It groups packets into separate classes on the basis of the type of service, and manages classes individually (as opposed to Integrated Services, which manages single connections). This policy provides the possibility to assign resources effectively, according to needs, but does not provide any service guarantees (for this reason, this service is also referred to as *soft QoS*). It just classifies traffic into service classes (this QoS scheme is often referred as CoS (Class of Service)), which allows preferential treatment of one over another. A service class represents a set of traffic that requires specific network characteristics from the network.

DiffServ distinguishes packets on the basis of DS Field (Type of Service (ToS) in IPv4 or Traffic Class (TC) in IPv6 - both are the size of 1 byte). That field consists of 8 bits in total - 6 left-most DSCP (Differentiated Services Codepoint) and lowest-order 2 bits for future use (currently unused), which makes it possible to define 64 traffic classes. Routers are allowed to change a packet's DS Field values to avoid a situation where all applications would have the highest priority assigned. The definition of the DS Field in IPv4 and IPv6 headers is provided in RFC2474.

The Differentiated Service architecture was developed by a part of IETFs IntServ working group, and defined in December 1998 in RFC2475. Configuration Guidelines for Diffserv Service Classes are provided in RFC4594.

Main DiffServ definitions are given below:

- **BA classifier** – an entity which selects packets on the basis of the DS field content,
- **Boundary link** – link between border routers in different domains,
- **Behaviour aggregate** – a set of packets with the same DS codepoint crossing a link in the same direction. The terms "aggregate" and "behaviour aggregate" are often used interchangeably,
- **DS boundary node** – a node connecting the DS domain with another network, with or without DS implemented,
- **(DS) codepoint** – a specific value of the DS field, it should map to specific, standardized PHBs. Multiple codepoints may be map to the same PHB.
- **DS domain** – a network over which a consistent set of DS policies are administered in a coordinated fashion. DS boundary nodes perform traffic classification and assignments to PHB groups.
- **DS egress node** – a boundary node which processes traffic incoming to/outgoing from the DS domain.
- **DS ingress node** – a boundary node which processes traffic incoming to the DS domain
- **Marker** – an entity which marks traffic with the DSCP code. It may also modify the packets existing DSCP code.
- **Multi-Field classifier (MF classifier)** – an entity which selects packets based on the content of packet headers, according to defined rules.
- **Per Hop Behaviour (PHB)** – describes the policy applied to a packet when travelling through a hop. The definition of PHB should be sufficiently detailed to allow the construction of predictable services, as documented in RFC2474.
- **Per Domain Behaviour (PDB)** – the expected treatment that an identifiable or target group of packets will receive from "edge to edge" of a DS domain. A particular PHB (or, if applicable, a list of PHBs) and traffic conditioning requirements are associated with each PDB.
- **Per Hop Behaviour Group (PHB Group)** – a set of PHBs with common constraints (e.g. queue servicing or queue management policy).
- **Shaper** – delays traffic by buffering packets to provide capability with the traffic profile. This action is also termed as traffic shaping.
- **Dropper** – drops traffic that does not comply with the traffic profile. This action is also termed as traffic policing.

- **Discard priority** – determines the order in which packets get discarded by a router, if unable to forward. Packets with higher discard priority are dropped before packets with lower priority.
- **Emission priority** – determines the order in which packets are forwarded by a router. Higher priority packets are sent before lower priority ones.
- **Assured Forwarding (AF)** – described in RFC 2597 PHB group, defines four independently forwarded classes, and three levels of drop precedence within each classes. A DS node is not allowed to reorder the packets in a particular AF class, irrespective of the drop precedence of the packet. Probability of packet drops grows with link saturation.
- **Expedited Forwarding (EF)** – described in RFC 2598 PHB, provides low loss, low latency, low PDV, assured bandwidth, end-to-end service through DS domains. This service is often referred to as Premium service, and is suits well VoIP needs. The recommended DSCP for EF is 101 110 00.

4.3. Congestion management

4.3.1. Standard TCP Congestion Control Algorithms

In RFC 2581 four congestion control algorithms were described: Slow Start, Congestion Avoidance, Fast Retransmit and Fast Recovery. These mechanisms monitor network traffic load to anticipate and avoid congestion at bottlenecks, which results in networks performance enhancements. The four TCP algorithms are described below.

4.3.2. Slow Start

Slow Start is a mechanism required for all TCP software implementation, used by the sender to control the transmission rate. Because of that it is also known as sender-based flow control. The sender can determine the sending bit rate on the basis of acknowledgements returned by the receiver. To implement this algorithm, two variables must be added to the TCP per-connection state – CWND (the congestion window), which determines the upper limit of data that the sender may transmit before receiving ACK (acknowledgment), and RWND (Receiver Windows), which defines the receiver-side limit on the amount of outstanding data. The CWND and RWND values determine transmission speed.

When transmission begins, Slow Start probes the network to determine the available capacity, and initializes a CWND with no more than two segments. The CWND grows proportionally to return acknowledgements – by one segment for each non – duplicate acknowledgement, which may double the maximum segment size, so the CWND will grow exponentially. It is worth noticing that the CWND value may (though it does not have to) be doubled, because several segments can be acknowledged by one ACK.

As link bandwidth is not infinite, increasing the data rate leads to congestion, where some packets must be dropped.

4.3.3. Congestion Avoidance

Congestion Avoidance technique is used in conjunction with Slow Start, but it aims to reduce transmission speed. This need occurs if congestion is present, typically indicated by receiving duplicate ACK (a packet is acknowledged more than once) or expiring the retransmission timer (no ACK delivered on time). If it occurs, the sender sets the Slow Start Threshold (SSTHRESH) value at half of the current CWND value (but to at least two segments). If congestion was indicated by timeout, the CWND is set to one segment and Slow Start mode is activated; if by duplicate ACK, the Fast Retransmit and Fast Recovery algorithms are started.

If data is delivered during Congestion Avoidance, the CWND is increased, in two ways – Slow Start is only used up to the halfway where congestion occurred (up to SSTHRESH value), and after that point by one for all segments in the transmission acknowledged. This policy is used to more slowly increase (approximately linear growth) the transmission rate up to the point where congestion occurs.

4.3.4. Fast Retransmit

Like Congestion Avoidance, the Fast Retransmit mechanism uses ACK to inform about network congestion. It assumes that if one or two duplicate ACKs are received, it is caused by packet reorder and the receiver can correct this problem. If more duplicate ACKs are present, the sender assumes that the packet was lost and shall immediately retransmit it. In that case, TCP switches to Fast Recovery mode.

4.3.5. Fast Recovery

If Fast Retransmit algorithm was in use when duplicate ACKs were received, the sender can assume that there is still some data flowing, and no serious network congestion occurs. So, instead of drastically reducing the CWND (by switching to Slow Start), the sender activates the TCP Congestion Avoidance mode.

4.3.6. Non-TCP congestion avoidance mechanisms

There are several congestion avoidance techniques not directly implemented within TCP, but with the ability to indirectly affect TCP congestion control mechanisms. The most important algorithms are described below.

4.3.7. Tail Drop

Tail Drop is a basic Congestion Avoidance mechanism. Queues are filling during congestion, and if buffers are full and there are still incoming packets, they are dropped. This technique does not differentiate between traffic classes – packet with high priority may be dropped in order to forward low-priority one, because both are dropped with the same probability.

The biggest disadvantage of Tail Drop algorithm occurs when buffer is full and all packets, particularly belonging to various flows are getting dropped. Senders went to Slow Start procedure, which causes dramatically decrease of incoming flow. As many hosts will be increasing and decreasing their transmission rates in the same timeframes, the link will not be efficiently used - waves of congestion and periods of time, when link will not be fully used will be formed.

4.3.8. Random Early Detection (RED)

The RED technique, proposed in early 1990's, is intended to provide considerable performance advantages with proactive approach to congestion. The basic assumption is that the most traffic is carrying data transport implementation, which will slow down the transmission rate if some packets are dropped.

RED controls the average queue size by randomly dropping packets if an average queue size exceeds the minimum threshold. The probability of packet loss grows proportionally to queue size and the proportion ratio may be set. Thus, a session with the largest CWND has highest probability to afflict data loss, and reduce the transmission rate as a result. This is intended to avoid appropriate link usage by a disproportionate large data flows. The non-deterministic packet drop policy avoid global synchronization problem, because at the beginning just a few flows losses data, and reduces transmission speeds. It might clear the congestion before queues are full and packets from all sources will have to be dropped. If the average queue size continues to rise, the packet loss probability grows slowly up to 100%, where all incoming packets must be dropped (just like in Tail Drop).

The main goals of RED mechanism are:

- to minimise the packets' delay variation,
- to strictly enforce the upper limit on the average queue limit,
- to avoid global synchronization problem,
- to support bursty traffic without bias.

As some protocols are very sensitive to data loss (like Novel NetWare or AppleTalk), RED shall not be used in networks based on those protocols. But, other protocols, such as TCP, respond appropriately to RED behaviour and slow down the transmission bitrates.

4.3.9. Weighted Random Early Detection (WRED)

The main imperfection of RED algorithm is lack of priority handling. As a result, high-priority flow has the same drop probability as low-priority, which may significantly decrease levels of services.

WRED is enhanced version of the RED algorithm, developed in aim distinguish traffic classes (e.g. on a basis of DSCP) and define various proportion rates. Thus, higher priority packets may be delivered with a higher probability than a lower priority one.

4.3.10. Queue

Queues are used to buffer excess packets before sending them through the network. In a perfect network, we would have unlimited bandwidth and unlimited forwarding rates, so there would be no need for buffers, but as those assumption often are unreal, we need to store or drop packets before sending. The most important scheduling algorithms are:

- **First In First Out (FIFO)** – basic scheduling policy; there is just one queue and packets are sent through the network in the order in which they appear. If the queue is larger than the buffer size, the last packets would be dropped. This scheme may be used only in Best Effort policy, because it cannot change the packet order in the queue and every packet is treated equally.

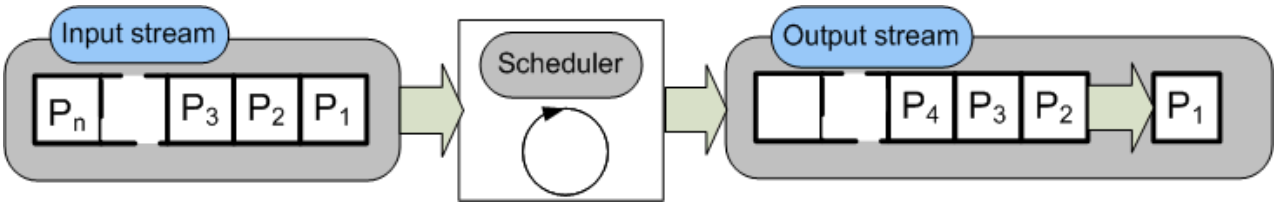

Figure 12 - Last In First Out (LIFO) algorithm

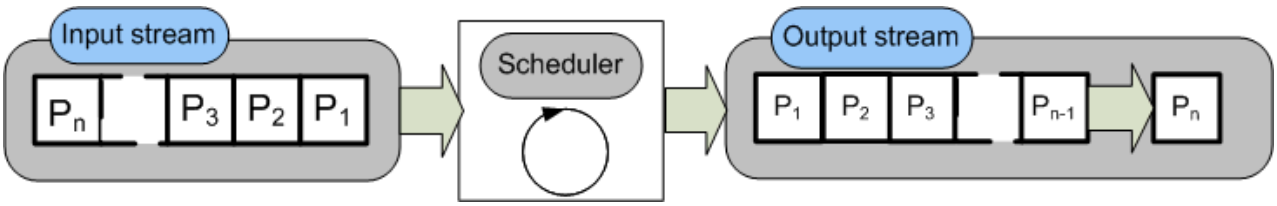

Figure 13 - First In Last Out (LILO) algorithm

- **Priority Queuing (PQ)** – has multiple queues, and allows the user to assign priority to them. Packets with the highest priority in queues are transmitted through the media; in case of several packets with the same priority the FIFO algorithm is used. As a result, the most important packet reaches the target before those with lower priority. On the other hand, low-priority packets may be blocked by higher priority ones, and as a result may not be delivered if a new high-priority packet arrives. In general, PQ is designed for networks where mission-critical data have the highest priority and it is possible to delay or drop less important data delayed during congestion. PQ is not compatible with the RSVP protocol.

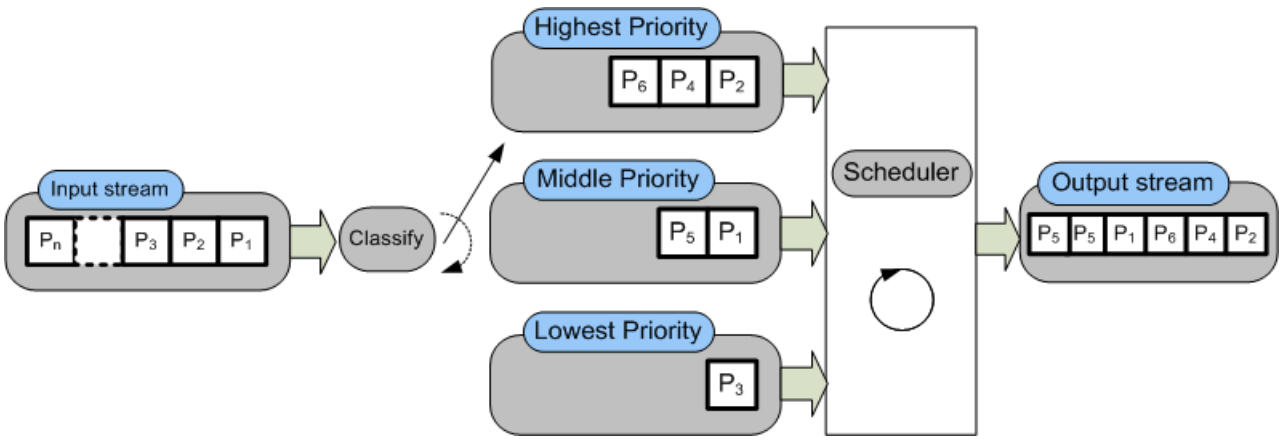

Figure 14 - Priority Queuing algorithm

- **Custom Queuing (CQ)** – packets are grouped into classes and available bandwidth is distributed proportionally between classes. The proportion ratio is configurable. CQ guarantees that mission-critical data have always at least a custom percentage of bandwidth available, and assures some throughput for other traffic.
  To achieve that, routers determine the maximum number of bytes that may be transmitted from the queue (on the basis of link throughput and class proportion ratio), and after transmitting it switch to the next queue in the round-robin fashion.

  It is worth mentioning that transmitted traffic can exceed the given limit in a particular round even during congestion, because if a packet size is larger than the remaining space, the whole packet will be transmitted. CQ is designed for networks where a minimal level of service is guaranteed to all protocols.

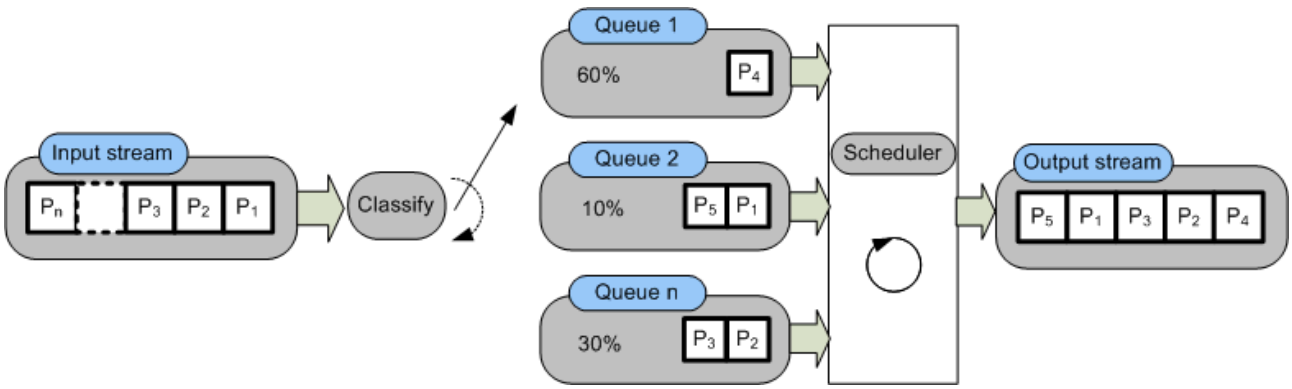

Figure 15 - Custom Queuing algorithm

- **Per Flow Priority Queuing (PFPQ)** – enhanced PQ mechanism; solves the problem where one flow can disallow other packets to be sent. In PFPQ, every flow has its own queue, and packets to sent are chosen in a round-robin fashion.

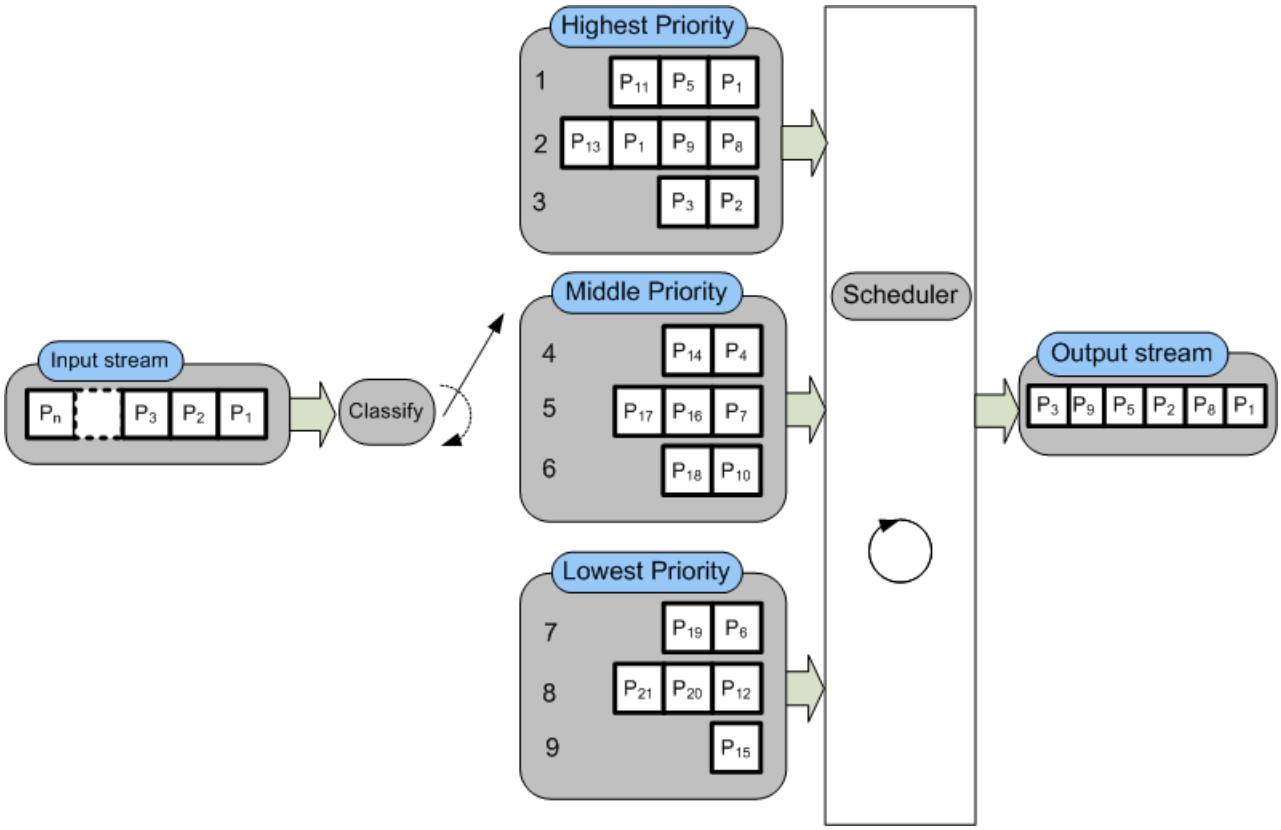

Figure 16 - Per Flow Priority Queuing algorithm

- **Weighted Fair Queuing (WFQ)** – flow-based queuing algorithm compatible with RSVP. Often used as a default in congested networks. Every flow has its own queue in the buffer, and the priority is proportional to the size of queue.
- WFQ is a basic algorithm, easy in configuration, but does not manage bandwidth and latency optimally. WFQ is also compatible with RSVP.

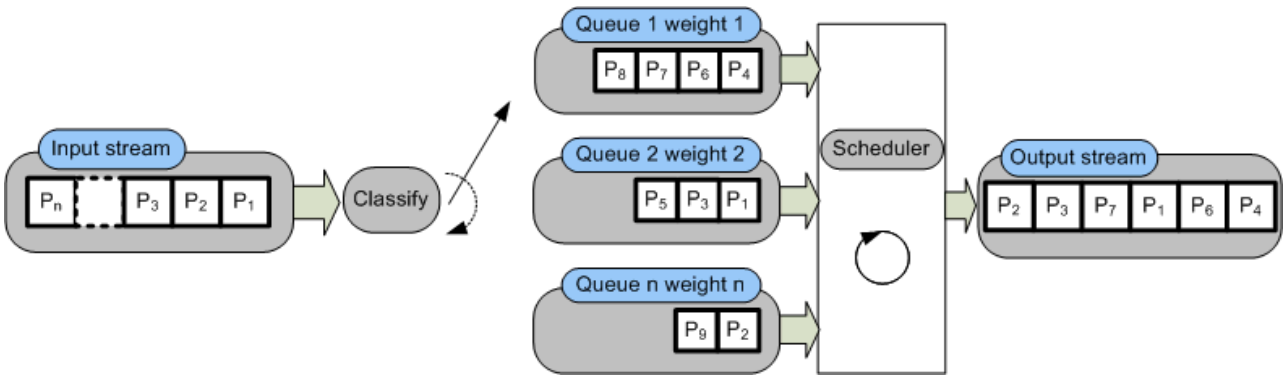

Figure 17 - Weighted Fair Queuing algorithm

- **Class Based Weighted Fair Queuing (CBWFQ)** – enhanced WFQ algorithm; every queue has an assigned weight (proportional to the queue length) and class, which defines relative participation in a bandwidth.

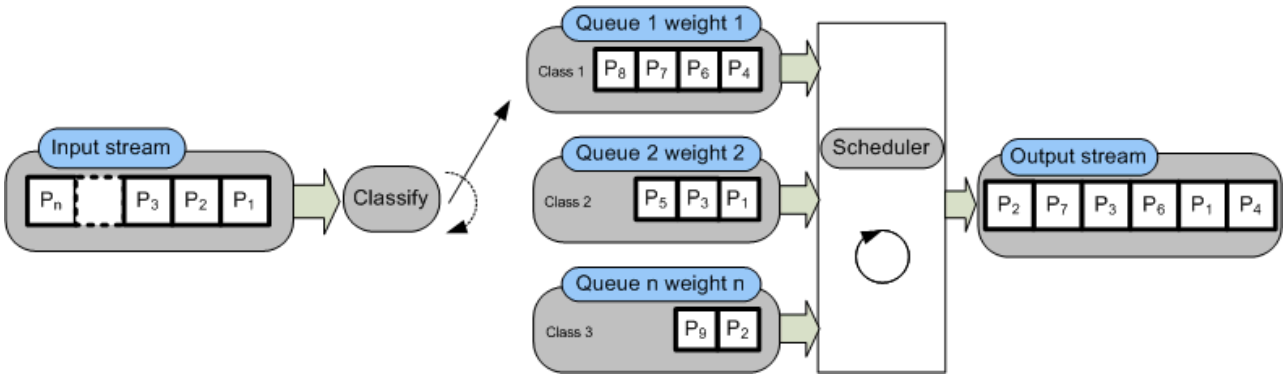

Figure 18 - Class Based Weighted Fair Queuing algorithm

- **Priority Queuing Weighted Fair Queuing (PQWFQ)** – enhanced WFQ algorithm; a special queue is present, which is always served first.

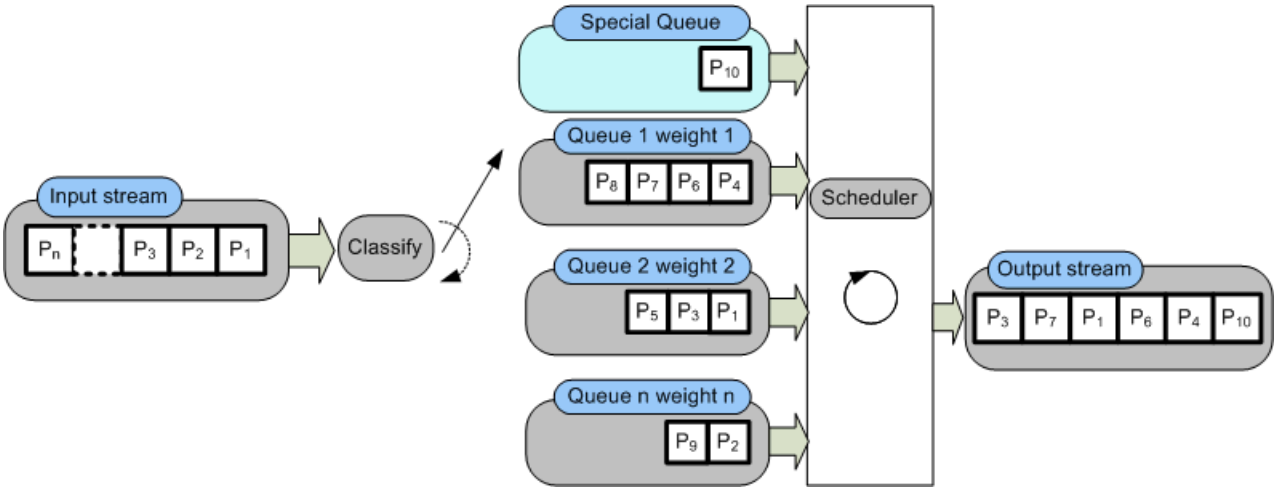

Figure 19 - Priority Queuing Weighted Fair Queuing algorithm

- **Priority Queuing Class Based Weighted Fair Queuing (PQCBWFQ) –** a merge of both above described methods (CBWFQ and PQWFQ). As a result, there are queues with assigned weight and class plus one first -served priority queue.

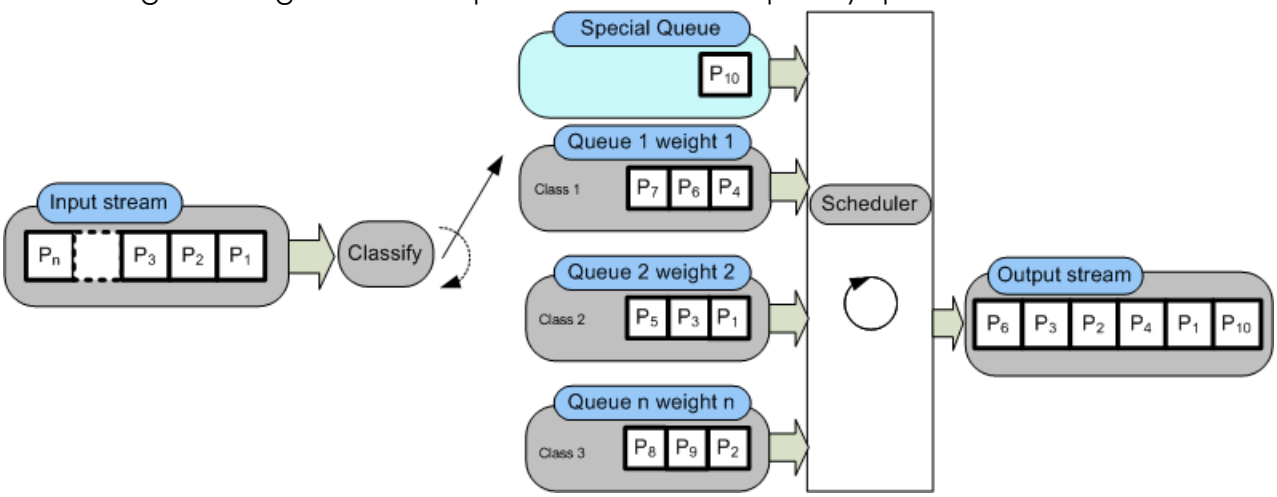

Figure 20 - Priority Queuing Class Based Weighted Fair Queuing algorithm

5. Session Initiation Protocol – SIP

5.1. Background

The Session Initiation Protocol (SIP), as it was mentioned in Deliverable 6.1 "Report on existing group call solution" is an application layer control (signalling) protocol for creating, modifying and terminating a session with one or more participants in Internet Protocol (IP) networks. Internet multimedia conferences, Internet telephone calls or multimedia distributions may be included in this session. The SIP can manage session initiation and invite members to a session. A session can be advertised using multicast protocols. Communications via voice, video or text may take place using any combination of SIP-enabled devices. Vendors increased incorporating SIP into their various IP communications products, including:

- WIFI phones,
- VoWLAN phones,
- wideband IP telephony,
- gateways, proxies and servers,
- PBX (Private Branch Exchange) systems,
- personal communications, instant messaging (IM) programs, softphones,
- audio and videoconferencing systems,
- wireless GPS EDGE systems.

5.2. Description

SIP is an application layer peer-to-peer communication protocol which works with IPv4 and IPv6 based networks. SIP is not a communication system and does not provide services. It is rather a component that can be used with other protocols to build a complete multimedia architecture and give basic functionalities to be used to implement different services. That is why SIP should be used in conjunction with other protocols in order to provide complete services to the users, i.e.:

- Real-time Transport Protocol (RTP) for transporting real-time data and providing QoS feedback,
- Real-time streaming protocol (RTSP) for controlling delivery of streaming media,
- Media Gateway Control Protocol (MEGACO) for controlling gateways to the Public Switched Telephone Network (PSTN),
- Session Description Protocol (SDP) for describing multimedia sessions.

However, the basic functionality and operation of SIP does not depend on any of these protocols.

SIP transparently supports name mapping and redirecting services which enable personal mobility. In telecommunications network services, this is defined as personal mobility, it allow end users to originate and receive calls and access subscribed telecommunications services on any terminal in any location and the ability of the network to identify end users as they move. Personal mobility is based on the use of a unique ID, i.e. personal number. Personal mobility complements terminal mobility. It means the ability to maintain

communications when moving a single end system from one subnet to another. ITEF has defined five aspects of establishing and terminating multimedia communications via SIP:

- user location: determination of the end system to be used for communication,
- user availability: determination of the willingness of the called party to engage in communications,
- user capabilities: determination of the media and media parameters to be used,
- session setup: "ringing", establishment of session parameters at both called and calling party,
- session management: including transfer and termination of sessions, modifying session parameters, and invoking services.

SIP's messages are easy to program and interpret, making it easier to achieve interoperability between disparate networks and different vendor solutions. SIP is also highly modular and extensible, allowing for integration with legacy systems and new and evolving technologies. Potential impact of SIP goes beyond internal communication. SIP has become a signalling standard for carrier networks.

5.3.Basic components

5.3.1.User Agents

SIP is modular composed, basic blocks that form the functions, i.e. user agents and SIP servers. The user agents represents an end systems, a user agent client (UAC) – applications installed on SIP endpoints, such as IP phone, mobile phone, wireless device or PDA or a laptop or desktop PC (see Figure 21) and a user agent servers (UAS) which generates responses to requests generated by UAC. UAC is capable of generating a request based on some external stimulus (e.g. the user clicking a button or a signal on a PSTN line) and processing a response. UAS is capable of receiving a request and generating a response based on user input, external stimulus, the result of a program execution or some other mechanism.

Figure 21 - Typical SIP user agents

When a UAC sends a request, the request passes through a number of proxy servers, which forward the request towards the UAS. When the UAS generates a response, the response is forwarded towards the UAC. UAC and UAS procedures depend strongly on two factors: first one based on whether the request or response is inside or outside of a dialog, and second one based on the request method. Dialogs represent a peer-to-peer relationship between user agents and are established by specific SIP methods, such as INVITE. Specifically, security mechanisms exist for the UAS and UAC to mutually authenticate each other. A limited set of privacy features are also supported through encryption of bodies using S/MIME.

SIP devices can communicate directly if they know each other's Uniform Resource Identifier (URI) or IP address, but more commonly, SIP servers are used in an enterprise network to provide an infrastructure for routing, registration, authentication and authorization services.

5.3.2.SIP Servers

SIP server is a server with combined functions, e.g. a RTC (Real Time Communication) server implements a proxy server and a redirect server on one server. Figure 22 presents basic SIP architecture.

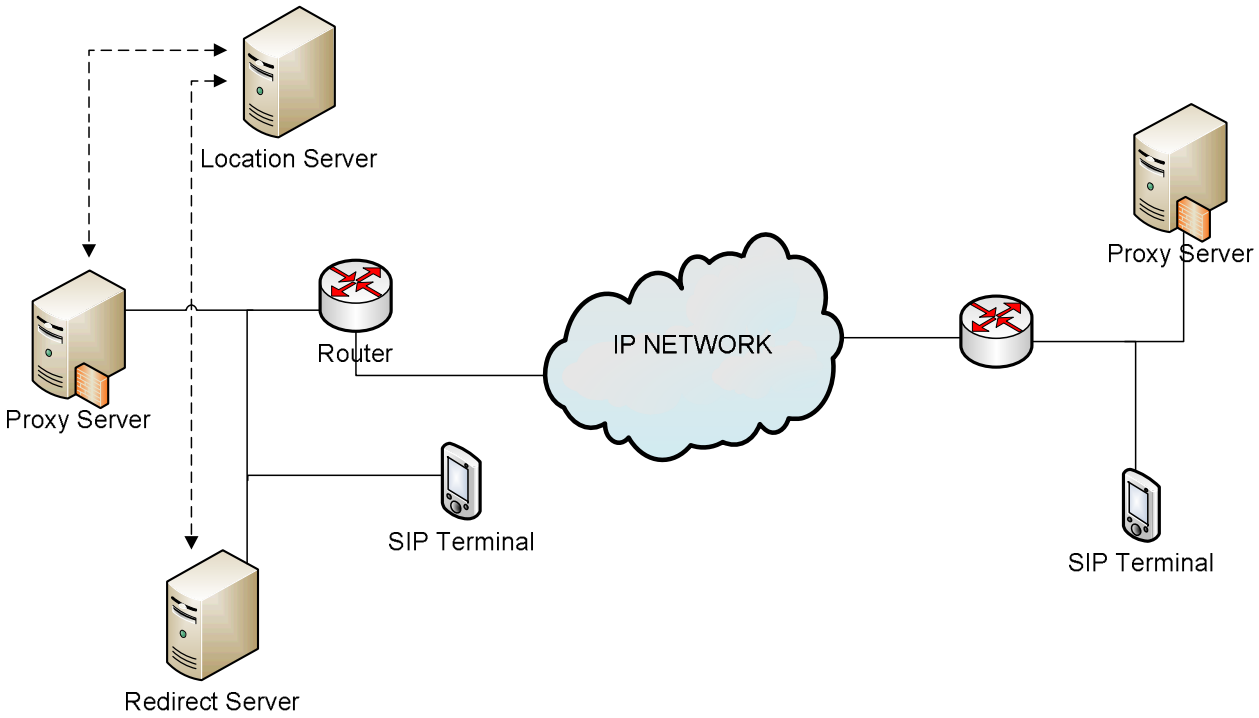

Figure 22 - SIP Architecture

SIP servers enable services in a SIP environment, which means that they provide centralized information about services. Determination of how the SIP messages will be processed, that is whether the messages go to the proxy or the redirect server, is performed through the configuration settings on the SIP server. Using this technology it is also possible to keep the service running while some of the servers are being worked on and/or maintained.

- **Registrar Server**

The registrar server authenticates and registers users when they come online and stores information on the users' logical identities and the communications devices of physical entities (IP address) of the communication devices they can use. The devices are identified by their Uniform Resource Identifier (URI). This server also makes possible for users to alter the address at which they can be contactable through the SIP client sending a REGISTER request of change of an address to the registrar server, which then accepts the request and records the user's new address. There are two ways in which the SIP clients can contact the registrar server. The first way is through a direct approach, by utilizing information that is configured into the client. The second way is through an indirect approach, which uses the multicast address to contact the registrar server.

- **Redirect Server**

The redirect server allows for redirection which enables users to temporarily change geographic location and still be contactable through the same SIP identity, e.g. if the user is not in his/her home domain, the session needs to be redirect to him/her. The redirect server maps a SIP request destined for a user to the URI of the device closest to

the user. This is the way that telephone communications enable the user (client) to be handed over from server to server as he/she moves around.

- **Proxy Server**

A proxy server takes SIP requests, processes them and passes them downstream while sending a response upstream to other SIP servers or devices. It works as a mediator that services the requests or forwards them to other UASs or UACs for servicing and may modify certain parts of a SIP request before passing it along. The proxy server can also be used for name mapping. That is, a proxy server can question a location service and map an external SIP identity to an internal SIP identity; it is involved only in the setup and tear-down of communication session. After user agents establish a session, communications occur directly between the parties. These proxy servers are not firewalls, they are independent servers on the Internet that proxy the request on behalf of the user for various reasons.

- **Presence Server**

Presence server accepts, stores and distributes presence information that allows users to see the availability of people they want to contact with. Presence server has two distinct sets of clients:

  - Presentities (producers of information)– provide presence information about themselves to the server to be stored and distributed
  - Watchers – receive presence information from server, can also subscribe certain addresses to users contact lists.

- **Back-to-Back user agent (B2BUA)**

B2BUA server can be a UA and the client server at the same time. The main role of this device is terminating the signalling from the calling UA, initiating signalling to the called UA. This server can change the content of a request, because of this it give them control over the call parameters.

- **Location Service**

An important service which is provided by SIP servers is the location service. It is a database that keeps track of users and their locations. The location service gets its input from the registrar server and provides key information to the proxy and redirect servers. A SIP proxy or redirect server uses this database to obtain the mapping from a logical SIP address to the physical SIP address. That is why the communication session can be properly established and maintained.

5.4.SIP protocol impact on the Secricom communication model.

SIP supports a new model for communications. Users can use the Extensible Messaging and Presence Protocol (XMPP, which can also be used for presence) and SIP for Instant Messaging and Presence Leveraging Extensions (SIMPLE). Both are widely adopted open protocol standards defined by IETF.

5.4.1.Presence

This feature is known in intelligent communication network as a possibility for a user to inform others about his/her status and on how he/she can be contacted before a communication session begins, thereby increasing productivity by making it easier to reach people efficiently. Users can specify their communications preferences and availability, which makes it easier for the calling side to reach a party that is available and wants to be called. Presence is not limited to a single person, it can also apply to a group of people or devices (e.g. medical operational group or decisions support managers group). Many devices, e.g. IP phones, mobile phones, softphones, wireless devices and PDAs, can provide presence information such as user status (online or offline), user availability (available or busy), user desired contact method (IM, phone, radio, etc.). SIP also uses presence to make routing decisions for a variety of incoming communications including routing urgent incoming calls and e-mail to others if the user is offline or taking part with operational actions. It can also route incoming calls from one device to another (e.g. from a PSTN phone to a mobile phone) if the user has indicated that he/she is roaming and prefers calls routed as such. Presence can be also used for classifying incoming communications as polite calls that the user can choose to answer, forward or ignore.

5.4.2.Modes of communication

Communications solutions converged with SIP enable users to interact with other or with an application in a variety of ways. Input can be via speech, keyboard, telephone keypad or mouse. Various modes of output may include synthesized voice, audio, plain text, motion video or graphics. SIP uses the Session Description Protocol (SDP) to determine what type of media stream the answering UA can support. SIP can make intelligent choices for modality. SIP-enabled solutions can handle:

- voice, video, Instant Messaging provided by common interface tied together with presence. Initiating communications is the same for each of these and the user can switch smoothly from one method to another.
- a SIP request originated by an English – speaking user might contain a Web services request to translate messages into another language for non-English speakers abroad. This service is named inline translation.
- In situations where the caller has only a phone and the called party has only a text device, transmission might be provided with text to speech and speech to text translation.
- A SIP enabled voice messaging system might provide features such as sending voice mail headers to the end user via text; sending virtual cards with every voice call so that other users from a group can have the caller's contact information available; playback, skip, rewind, pause, shut down and speedup buttons available with a graphical interface in a screen device.

5.4.3.Streamlining communications architecture

SIP communications architecture consists primarily of SIP endpoints and SIP servers. In small networks it can be simplified and allow to reduce associated costs by direct communication between intelligent endpoints. User agents can be programmed to

communicate with others without servers, this way of communication is called peer to peer SIP communication (P2PSIP). P2PSIP effectively replaces the registration, location and lookup steps in SIP.

5.4.4. SIP mobility

SIP is well suited for mobile environments. Registration functions are similar to that in GSM and 3GPP (Third-Generation Partnership Project) networks. When a user turns on SIP devices, it registers the user and sends the devices to URI (Uniform Resource Identifiers) to the register server which routes calls to and from users. This system ties together communication using a single address that can reach the user regardless of location. Further facility of SIP URI is to support both numeric and alphanumeric formatted contact addressing, thanks to which the public switched telephone network (PSTN) and the Internet can be seamlessly linked together. Native mobility is the reason that 3GPP has adopted SIP as its primary signalling protocol for the IP Multimedia Subsystem (IMS). Furthermore, SIP includes simplicity, flexibility, extensibility and familiarity as the core technology for supporting IMS. IMS provides a framework enabling rapid development of innovate multimedia applications and content over a mobile network.

5.4.5. Trunking with SIP

SIP trunks enable to carry voice data over an IP connection to carrier clouds. A SIP proxy peers with a carrier SIP proxy, with the appropriate federations and security protections established between them. The IP circuit continues to carry data and other traffic as it usually does. SIP sets up and tears down data connections to and from users over this IP circuit. On – net calls traverse the carrier's VoIP backbone (which is dedicated to voice to guarantee voice quality). Off – net calls ride the carrier IP network until a gateway converts VoIP to TDM for calls to PSTN parties. In a converged network, voice becomes an IP application, sharing the common network infrastructure and services.

5.5. Quality of Service and SIP

SIP does not support Quality of Service itself, since it has no mechanism which could support QoS in pure form. Basically, a form of resource reservation may be needed. According to IETF resources, the SIP users agents should rely on existing QoS protocols for support of such resource reservation (e.g. RSVP protocol). This option has two drawbacks:

- the user application must be aware of QoS mechanism used (e.g. RSVP, COPS etc.),
- user application must implement QoS protocol used to assure those mechanism (e.g. if RSVP is used as a signalling protocol ,user terminals should implement the RSVP protocol).

Basically, there are two QoS models possible, in which:

- **QoS** is **assured**, i.e. the session should not be established if resources are not available,

- **QoS** is **enabled**, i.e. the session is established regardless of the availability of QoS resources.

5.5.1. QoS scenario and architecture in SIP network

The figure below (Figure 23) presents the quality of service scenario in SIP networks. The SIP terminals are connected to the Core Network, in which QoS is supported, via Access Points. The Access Points at the border of such network can provide QoS mechanism to SIP terminals. The QoS at the access networks depends on the QoS model used by the ISP for the access.

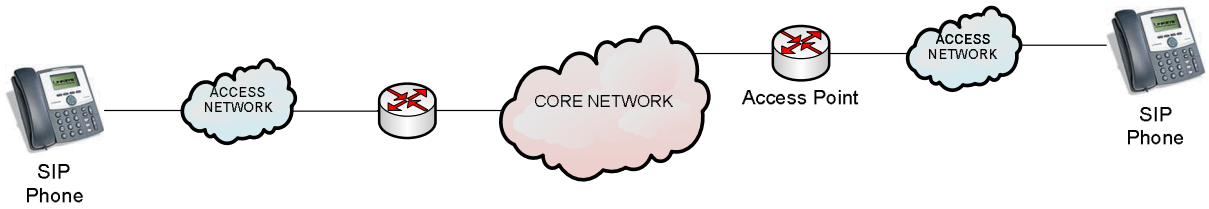

Figure 23 - Reference QoS scenario

The idea of supporting QoS in SIP networks is to use SIP proxy servers for SIP UAs in their domains for incoming and outgoing calls. The UA sends and receives SIP messages to appropriate proxy servers. The SIP servers can add QoS information in the SIP message and send it forward (what is meant as an offer to terminating SIP server to contact with QoS support). The SIP session will be setup with QoS because the terminating SIP server will understand the QoS information in the SIP message. The SIP servers are also involved in message exchange which is invisible for UAs. The network QoS mechanisms can interact with the SIP QoS parameters extracted from messages.

Figure 23 and Figure 24 present two supporting QoS architectures. The quality of service provided by this type of network is located at the border of the network in the QoS Access Points. Depending on the mechanism implemented inside the core network, there can be two types (logical types) of QoS Access Points with various reservations, e.g. unidirectional and bidirectional form an accession to Access Points. In the first proposed architecture, two different reservations have to be requested to the QoS network (the RSVP QoS model also works this way). When we talk about bidirectional flow reservation, the difference is that we have a single QoS Access Point and a single reservation request made by the QoS enabled SIP server.

Figure 24 presents a proposition of a QoS architecture in which the need of QoS support was eliminated on the user terminals since all the QoS functions can be moved to local SIP servers that will control call setup and resource reservation. When call setup is initiated, the caller SIP UA can start a SIP call setup session established through a proxy server. QoS enabled SIP server starts a QoS session interacting with a remote QoS enabled SIP server and QoS provider (QoS Access Point). The data session starts when the QoS provider responds and call setup can be continued. The QoS setup procedure is based on QoS aware agents - SIP servers. Protocol extensions required for this process are hidden and not visible for SIP agents which are not aware of the QoS support mechanisms.

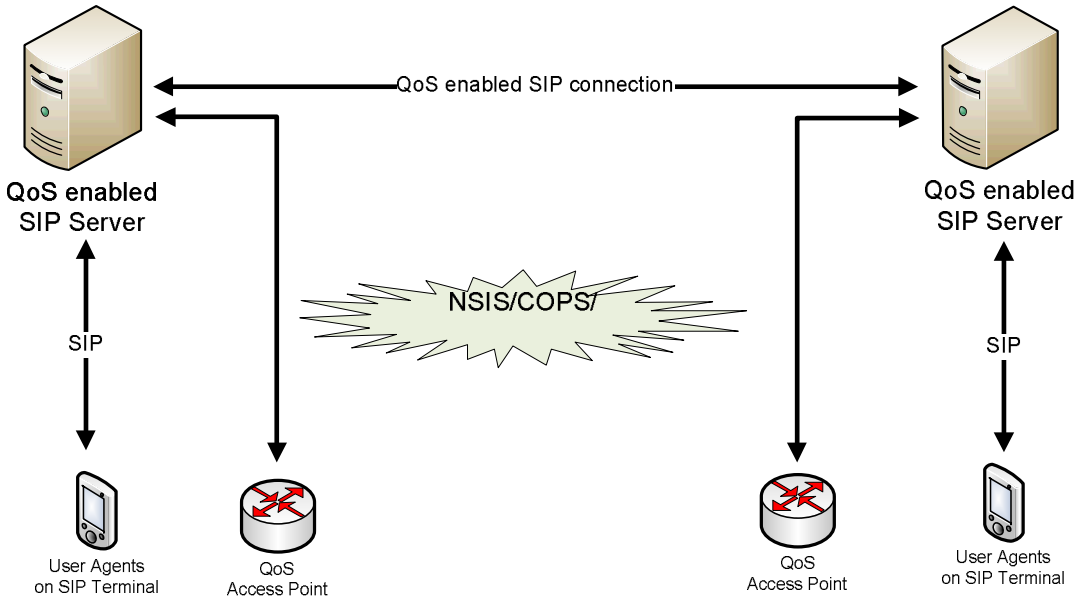

Figure 24 - QoS enabled SIP server architecture with unidirectional flow reservation

Basically the requirements of the QoS enabled SIP servers are:

- possibility of using existing SIP UAs,
- possibility of seamless interaction with other parties which are not able to use QoS,
- the protocol enhancement should preserve backward compatibility with standardized SIP protocol,
- simple resulting architecture,
- scalable resulting architecture,
- extensible architecture to new QoS supporting models of IP networks.

The process of setup QoS supported session is composed of two parts: the end to end signalling mechanism to exchange information (generic and independent from the QoS mechanisms) and the QoS negotiation between SIP UAs and QoS network (core network).

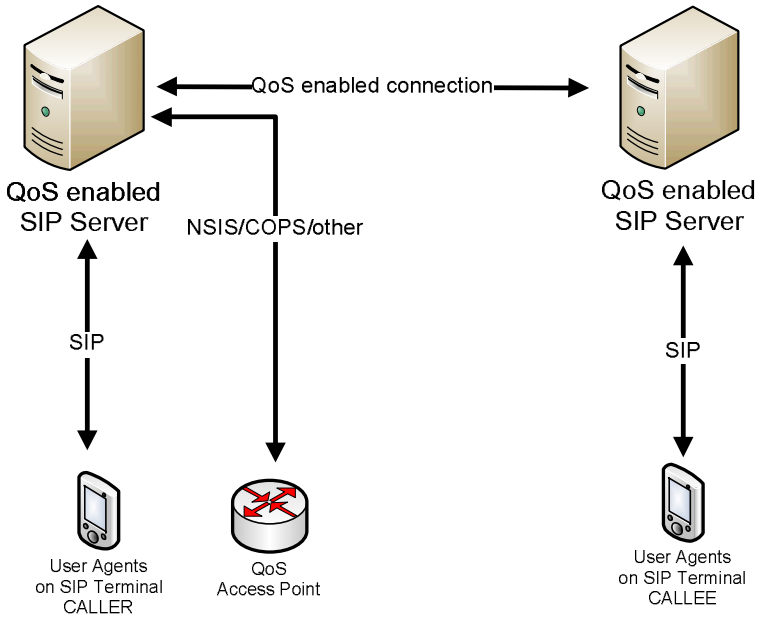

Figure 25 - QoS enabled SIP server architecture with bidirectional flow reservation

The proposed mechanism can be also applied to a scenario where the SIP UAs can support QoS aspects (QoS aware UAs) which support SIP servers. In that case, the QoS enabled architecture would be like that on Figure 26.

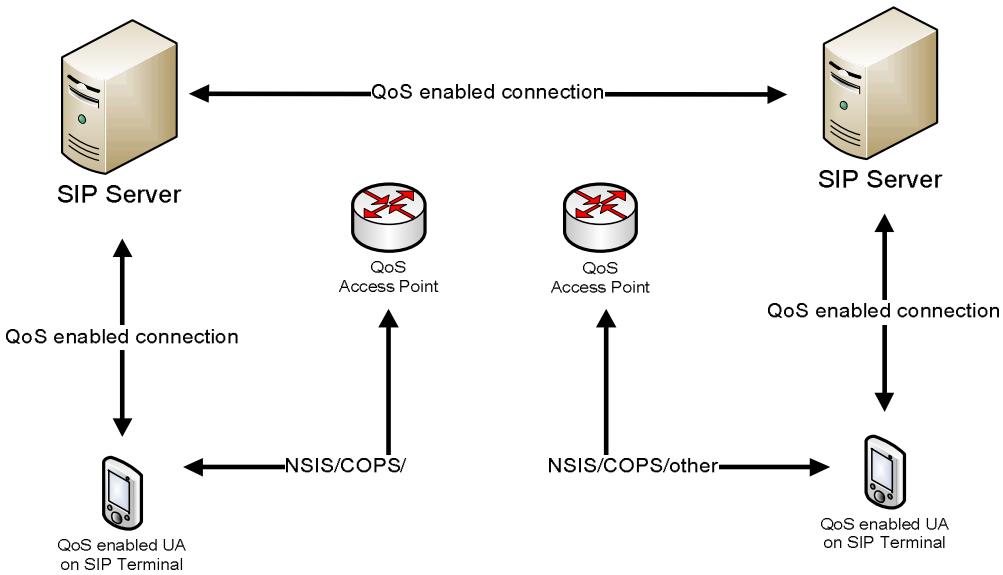

Figure 26 - QoS enabled architecture with QoS enabled agents on terminals

5.6. SIP security

Considering security aspects, it is needed to recognise user requirements depending on specificity of the exchanged data. There are various security targets and objectives in a

SIP network. It is important to clearly define what needs to be secured and against what. The user requirements can be specified as:

- the need to ensure authentication which means mutual authentication (both users) before accepting incoming calls to see who is calling.
- the need to ensure data confidentiality and integrity, which means that third parties cannot tap the conversation.

For the purpose of this discussion is defined several cases of connection between communication parties. For authentication, encryption and integrity they are:

- UA to UA mutual authentication. Both (caller and callee) should authenticate themselves and the user should have information on who is calling. Encryption is sent with confidentiality.
- UA to B2BUA – the UA (client) should authenticate itself to the SIP server (B2BUA). It is known as first mile protection, necessary when using untrusted access network.
- B2BUA to UA – the UA (client) must authenticate the server (B2BUA). UA should know to whom it is sending the credentials.

Basically SIP and RTP standard has no implemented security mechanism but it is possible to deliver it by other protocols, e.g. TLS, IPSec, MIKEY, etc.

5.6.1.SIP build-in security mechanisms

To assure the right access control and availability of the service, the request for the possible QoS session should be authenticated. Additional proxy authentication should be used to assure the correct handling of the QoS service offered to the agents (UAs) by the QoS enable server. The user profile might contain user password and the type of service for which the user is enabled, it could be use as authentication and resource reservation support. Even SIP standard provides some possibility to authenticate transmission, SIP digest authentication is the most spread security technique for UA to B2BUA authentication.

5.6.2.SIPS with SRTP

SIPS is the SIP communication protected by the TLS protocol. It can be used only to protect SIP signalling and not the RTP data, because TLS is defined over TCP. This option can be used with authentication unidirectional e.g. UA to B2BUA or B2BUA to UA. Additionally for authentication x509 certificates can be used but it is an elaborate problem to manage of many user certificates. Simple way is to use only TLS for B2BUA to UA without client certification. For UA to B2BUA authentication, username and password can be used (MD5 digest authentication is a part of SIP standard). In one case the authentication and protection cannot be achieved – when there is no direct network layer connection between the UAs. It is possible only in UA to UA authentication.

Since TCP session cannot be established from outside NAT device, SIPS cannot protect incoming calls from dynamic NAT environments. SIPS currently can protect only outgoing sessions.

Providing the key generation mechanisms must be delivered by other protocols. SIP or SRTP either do not provide it. In this case the key can be delivered by key attribute in SDP. The key can be send clear because the lower TLS layer protects signalling session.

There is another consideration defined in RFC standards. It is called "hop by hop" which means that only connection between the nodes is protected and in the nodes data is in clear form. Each server node can read and modify the signalling packet because the chain of trust is build hop by hop. It is not acceptable for end-to-end communication because the client cannot influence the trust decision in the next hops. In this case it can happen that not every node will trust to other one but can be in the chain trust. This happens when there is a difference status between the nodes, e.g. the UA caller do not trust the inbound proxy of the UA callee but trust its own outbound proxy. If the outbound proxy trusts the inbound proxy the trust chain can be established.

The conclusions are, that SIPS with SRTP are not recommended for end-to-end user authentication with SIPS. This combination is an alternative for protecting outgoing calls in the first mile UA to B2BUA. Incoming sessions are not protected, when the UA (user) trust the hop-by-hop principle the SIPS and SRTP can be established between end clients.

5.6.3.IPSec

The basic role of IPSec was described in D6.1 deliverable 'Report on existing group call solution', where was described how to enhance the security level in IP networks. The advantage for IPSec is that one session can assure protection SIP and RTP and any other protocol if it is adjustment to IPSec.

Since the B2BUA and SIP proxy must read and transform the SIP, the UA to UA protection cannot be made. IPSec encrypts the SIP header that is why they cannot be read between B2BUA and proxy server. Additionally TLS protection is present. Whole that makes the IPSec a good alternative for securing the first mile UA to B2BUA. The protocol provides mutual authentication on B2BUA and UAs using certificates, optional combined with password authentication in SIP.

5.6.4.SMIME with SRTP

Combinations of those protocols give possibility for secure the SDP and SIP payload. The SMIME allows mutual authentication UA to B2BUA using SDP payloads with cryptographically signatures verification and matching the ID in the sender certificate with SIP header. It can protect session hijacking when the SIP header is signed. This process can be done by tunnelling SIP headers in the SDO payload.

In UA to UA sessions, the whole SDP payload cannot be encrypted in SMIME. The intermediate devices (SIP servers: B2BUA and proxy) need to edit at least the RTP contact parameter. Encryption is assured by Key-attribute in the SDP which contains the protection key for the SRTP. This option assures secure end-to-end transmission and servers can process the SIP packets.

Conclusion is that use of SMIME make sense with authentication between the clients, it is not recommend for server to user (B2BUA to UA and UA to B2BUA) authentication.

5.6.5. MICKEY with SRTP

MICKEY is a key exchange algorithm. It can be used for user authentication and key derivation for SRTP and does not have many encryption parameters. Messages send using MICKEY are embedded in SDP attributes what allows the key exchange without additional packets. Algorithm offers three exchange modes:

- shared secret – clients (UA caller and UA callee) are authenticated using a share secret,
- public or private key encryption – UA caller (initiator) generates and signs the session key and the UA callee (responder) must be known in advance,
- *Diffie–Hellman* with signatures – key exchange and certificate advantages are used (PKI infrastructure needed) and involved existing CA authorities. This option is the most recommendable alternative in MICKEY.

MICKEY with SRTP is reasonable solution for end-to-end client authentication and RDT protection but it cannot be used for UA to B2BUA protection.

6. Preparation for Demonstration and Dissemination

6.1.Background

Within the description of work for Project SECRICOM at Task 6.4 is a requirement for the 'Preparation of a Demonstration and Dissemination'. As one of the first steps in the path towards a final project demonstrator test it is planned that IVP6 technology, which form part of the overall final solution, will be tested in a simulated Civil Protection related crisis environment.

The University of Luxembourg in its role of WP6 lead has arranged for a sample IPv6 based PTT group call to be exercised as well as showing the Secricom modules of communication; it plans to work in cooperation at an exercise with the Slovak Civil Protection in September 2010. Results will be published through the Project's dissemination activities and will include IPv6 related forums (IPv6 Forum, EU IPv6 Task Force, etc.).

The context of this planned IPV6 test and indeed all future demonstrator tests is shaped by the agreed Project Approach as illustrated in Figure 27 below. As can been seen from the diagram central to the overall demonstrator test programme is the Project Scenario.

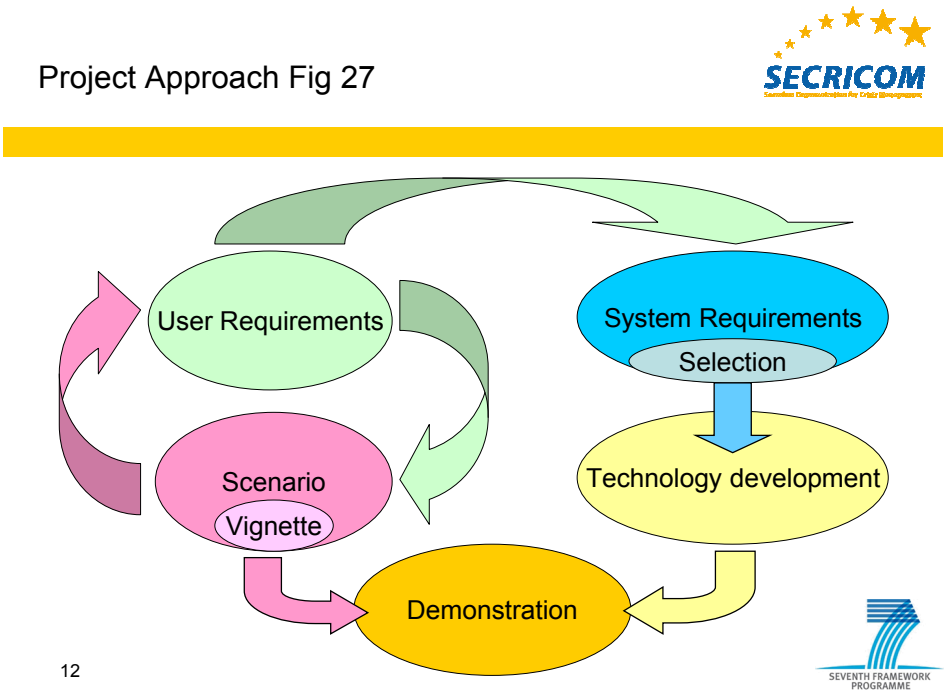

Figure 27 – Project Approach

6.2. The Scenario

The Project scenario is fundamental in shaping User and System Requirements. Subsequent decisions around specific technology development that will be exercised in the Demonstrator Test programme will be further informed by the selection of a vignette or sub set of the overall scenario and an associated case study exercise that leads to key information exchange requirements (IERs). These IERs will shape the evaluation criteria of all Project demonstrator tests to ensure that it will be user requirements enabled by the new developed technology that are proved.

The Project scenario is based around a plausible situation as regards a reservoir that has retaining walls that are likely to breach; under threat is an urban area that includes various transport and communications infrastructure also a chemical plant. When the reservoir wall breaches the incident encompasses a neighbouring country. For a full description of the scenario please see Annex 1

In developing the scenario the Project User team listed various assumptions that shaped their contributions. Since the completion (May 2009) and validation of the scenario (by Civil Protection managers in Luxembourg and Slovakia) a key assumption has been updated as follows:

- The UK major event management doctrine utilised within the scenario of strategic, tactical and operational levels of command is similar to other European emergency/civil protection agencies - validated in Luxembourg, Slovakia and Sweden (Summer and Autumn 2009)

6.3. Project Scenario Vignette - Chemical Plant Noxious Smoke Cloud

In accordance with the agreed Project Approach (Fig 26) a vignette of the overall project Scenario has been developed – a Chemical Plant Fire and Noxious cloud.The following is the outline for the project vignette; this should be read in conjunction with the overall project scenario (Annex 1)

'It is at this point information comes to light through rumors at working level that the chemical plant illegally had on its premises large quantities of unlicensed and dangerous chemicals and that it had failed to remove them from the plant in time; shortly after there is a large explosion at the plant and a massive plume of smoke is seen originating from the chemical plant.

This smoke plume forms into a large toxic gas cloud and with the northerly wind starts to spread the plume over into country B. Chemical plant management own up about the illegally stored chemicals. Expert advice on the chemicals held at the plant suggests this toxic gas cloud will be harmful to people with the elderly and the young at greatest risk - possibly fatal. The plume is monitored by Country A's helicopter with live video feed to ground based control rooms

Some of the dead and injured are displaying particular types of body burns indicative of being in the vicinity of the chemical plant and in particular the toxic gas cloud; health agency advice is needed before rescuers and body recovery teams can deal with them on both sides of the international border.

The following key activities are agreed at the multi-agency strategic co-ordination level

- *Containment of this particular incident*
- *Preservation of Life – members of the public*
- *Preservation of Life – first responders involved in incident*
- *Protection of Environment*
- *Preservation of Evidence for subsequent enquiry/prosecution*
- *Maintenance of good diplomatic relations with neighbouring country*
- *Preservation of public order'*

These key activities are arranged as follows and are consistent with top level requirements for any major incident or crisis.

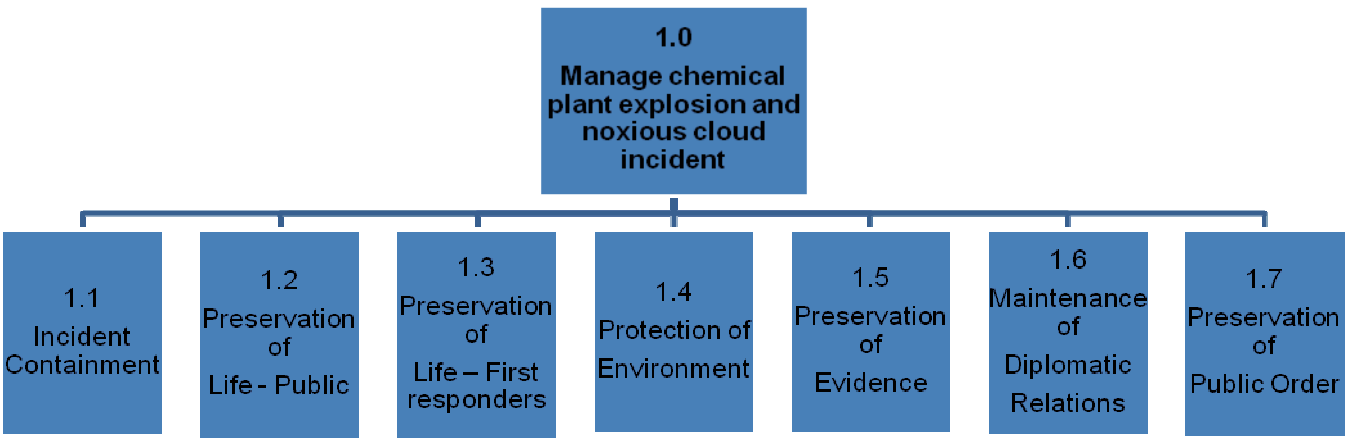

Figure 28 - Noxious cloud incident

Following on from the vignette a case study exercise has been developed with a core project team of users under the WP10 programme of activity.

6.4.Project case study - Chemical plant fire & noxious cloud

The Case Study exercise identified a wide range of information needs necessary for a Civil Protection Agency to conduct operations in response to a major incident. The exercise developed detailed flow charts of need for each of the key activities highlighted (1.1 through to 1.7); for a full breakdown of the Case Study Charts see Annex 2. The Case Study also enabled the development of detailed information exchange requirements (IERs) i.e. the identification of specific communication needs in terms voice or data, priority and length, and several other qualifying criteria. This work is still under development in WP10.

WP6 has selected the 1.3 requirement – Preservation of Life for First Responders – as the basis of the planned IPV6 test to be conducted with the Slovak Civil Protection in September 2010. It is intended that the detailed information exchange requirements identified in the current WP10 will shape the specifics of the test and evaluation criteria for the IPV6 enabled demonstrator with the Slovak Civil protection.

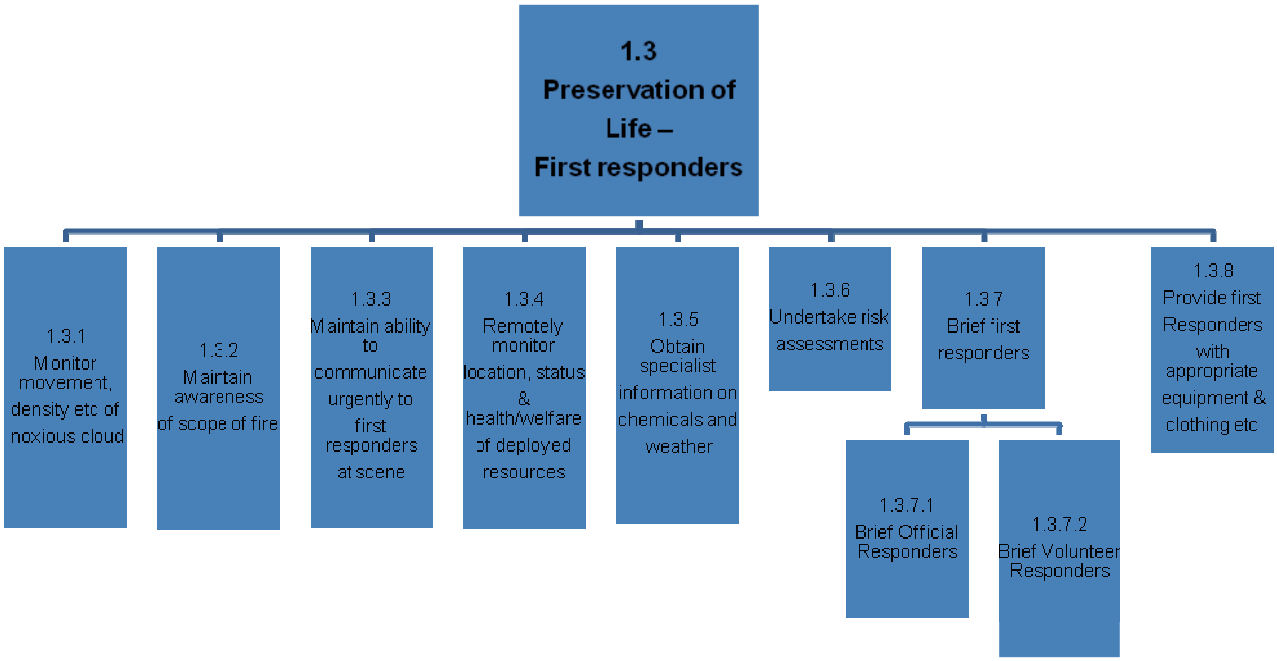

Figure 29 - Preservation of Life – First responders

7. Conclusion

In this Deliverable, we have presented IPv6 based secure communication to have the overall picture of functionality of communication modules of the Secricom solution. The work done in this deliverable covers the Tasks mentioned in the Work Package 6 of Description of Work of project Secricom. It is not just theoretical work. We are aware that IPv4 spaces are running out. The project has progressed the work on partial modules of the Secricom communication solution. We have begun to prove particular modules that were normally working over IPv4 spaces in the IPv6 environment. In doing this the project has achieved the goal to be ready for future IPv6 Internet and IPv6 based communication in the crises situation.

The security part of this Deliverable has identified the security problems in the case of using IPv6 protocol. The Secricom solution will have to prepare QoS standards about what is done and these are recorded in Chapter 3.

The D6.2 Deliverable proved the modules of Secricom communication solution for Public safety in the laboratory tests and gave vision of work in the IPv6 space. The second phase will follow with a demonstration where we will simulate a vignette based on the crises scenario mentioned in Chapter 5. The project will use modules for data and voice communication in a simulated crises condition and with IPv6 communication protocol.

References

- IPv6 Security – Information assurance for the next generation Internet protocol; Scott Hogg
- IPv6 and IPv4 Threat Comparison and Best-Practice Evaluation; Sean Convery and Darrin Miller http://www.cisco.com/web/about/security/security_services/ciag/documents/v6-v4-threats.pdf
- IP Dual Stack Security Implications; Sean Convery and Darrin Miller http://seanconvery.com/Internet2.pdf
- The Ghost in Your Machine: IPv6 Gateway to Hackers; Kim Zetter http://www.wired.com/threatlevel/2008/07/the-ghost-in-yo/
- IPv6 Internet Security for Your Network; Eric Vyncke and Scott Hogg http://www.informit.com/articles/article.aspx?p=1312796
- Security Implications of IPv6; Michael H. Warfield http://documents.iss.net/whitepapers/IPv6.pdf)
- IPSec&IPv6 – Securing the Next Gen Internet; Kaushik Das http://ipv6.com/articles/security/IPsec.htm
- Secure Neighbor Discovery (SEND); Lakshmi http://ipv6.com/articles/research/Secure-Neighbor-Discovery.htm
- Enabling Network Mobility: A survey of NEMO; Paul Moceri http://www.cse.wustl.edu/~jain/cse574-06/ftp/network_mobility/index.html
- Network Mobility Support in IPv6 (NEMO); Thierry Ernst http://portal.unesco.org/ci/en/files/19999/11272932761ernst.pdf/ernst.pdf http://oss.oetiker.ch/mrtg/ http://www.cisco.com/en/US/products/ps6601/products_ios_protocol_group_home.html
- RFC 3261 "SIP: Session Initiation Protocol"
- RFC 2246 "The TLS Protocol"
- RFC 2401 "Security Architecture for the IP"
- RFC3830 "MICKEY: Multimedia Internet KEYing"
- RFC 3711 "The Secure Real – time Transport Protocol"
- RFC 1889 "RTP: A Transport Protocol for Real Time Applications"
- RFC 3263 "SIP: Locating SIP Servers"
- RFC 2026 "SIP Extensions for QoS support"
- RFC 1633 "Integrated Services in the Internet Architecture: an Overview
- RFC 2460 "Internet Protocol, Version 6 (IPv6). Specification"
- RFC 2474 "Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers"
- RFC 2475 "An Architecture for Differentiated Services"
- RFC 2597 "Assured Forwarding PHB Group"
- RFC 2598 "An Expedited Forwarding PHB"
- RFC 3393 "IP Packet Delay Variation Metric for IP Performance Metrics (IPPM)"
- RFC 2205 "Resource ReSerVation Protocol (RSVP) - Version 1 Functional Specification"
- RFC 2208 "Resource ReSerVation Protocol (RSVP). Version 1 Applicability Statement. Some Guidelines on Deployment"

- RFC 3697 "IPv6 Flow Label Specification"
- Young-Chul Jung, Jong-Chul Seo and Young-Tak Kim - "Session &Connection Management with SIP and RSVP – TE for QoS-guaranteed Multimedia Service Provisioning"
- Sang-Jo Yoo, Nada Golmie, Haolang Xu "QoS-Aware Channel Scanning for IEEE 802.11 Wireless LAN"
- 6th International Workshop "Passive and Active Network Measurement"
- R. Yasinovskyy; A. Wijesinha, R. Karne, G. Khaksari - "A comparison of VoIP performance on IPv6 and IPv4 networks"
- Athanassios Liakopoulos, "QoS experiences in native IPv6 GRNET and 6NET network"
- WilliamC.Hardy "QoS Measurementand Evaluationof TelecommunicationsQuality of Service"
- Adrian Farrel "Network Quality of Service Know It All"
- Srinivas Vegesna "IP Quality of Service"
- Cisco "Internetworking Technologies Handbook" http://www.cisco.com/en/US/docs/internetworking/technology/handbook/ito_doc.html
- Implementing Quality of Service Policies with DSCP http://www.cisco.com/en/US/tech/tk543/tk757/technologies_tech_note09186a00800949f2.shtml