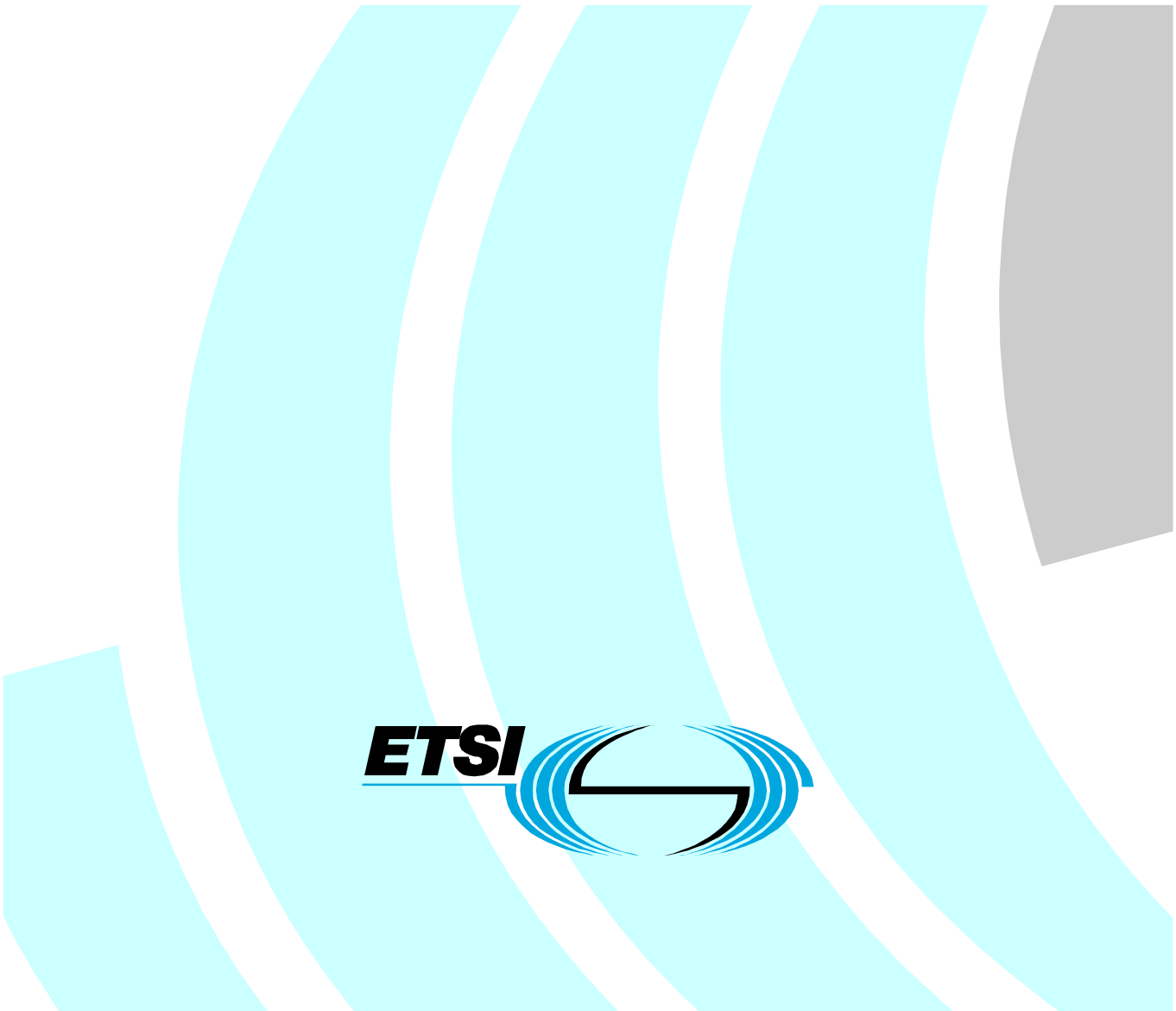
ETSI TR 102 419 V1.1.1 (2005-04)

Technical Report

Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Security analysis of IPv6 application in telecommunications standards



Reference
DTR/TISPAN-07001-Tech

Keywords
IP, security, telephony

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Contents

Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (http://webapp.etsi.org/IPR/home.asp).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Foreword

This Technical Report (TR) has been produced by ETSI Technical Committee Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN).

1 Scope

The present document provides an analysis of the security provisions made in IPv6 and outlines how they may be used to support the objectives of the European Commission to support the implementation of PKI solutions and the further deployment of IPv6 and IPsec.

2 References

For the purposes of this Technical Report (TR), the following references apply:

[1] "Overhead Issues for Local Access Points in IPsec enabled VPNs", John Ronan, Paul Malone, Mícheál Ó Foghlú, Proceedings of IPS Workshop, Salzburg, February 2003.

[2] TORRENT (Technology for a Realistic End User Access Network Test-bed), IST-2000-25187. http://www.torrent-innovations.org.

[3] IETF RFC 2410: "The NULL Encryption Algorithm and Its Use With IPsec".

[4] Andrew Tannenbaum: "Computer Networks (International Edition)"; Prentice Hall PTR; ISBN: 0130384887.

[5] ETSI SR 002 211: "List of standards and/or specifications for electronic communications networks, services and associated facilities and services; in accordance with Article 17 of Directive 2002/21/EC".

[6] Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive.

[7] IETF RFC 2460: "Internet Protocol, Version 6 (IPv6) Specification".

[8] IETF RFC 793: "Transmission Control Protocol".

[9] IETF RFC 768: "User Datagram Protocol".

[10] IETF RFC 2326: "Real Time Streaming Protocol (RTSP)".

[11] IETF RFC 1889: "RTP: A Transport Protocol for Real-Time Applications".

[12] IETF RFC 2474: "Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers".

[13] IETF RFC 2475: "An Architecture for Differentiated Service".

[14] IETF RFC 2205: "Resource ReSerVation Protocol (RSVP) -- Version 1 Functional Specification".

[15] IETF RFC 2206: "RSVP Management Information Base using SMIv2".

[16] IETF RFC 2207: "RSVP Extensions for IPSEC Data Flows".

[17] IETF RFC 2208: "Resource ReSerVation Protocol (RSVP) -- Version 1 Applicability Statement Some Guidelines on Deployment".

[18] IETF RFC 2209: "Resource ReSerVation Protocol (RSVP) -- Version 1 Message Processing Rules".

[19] IETF RFC 2210: "The Use of RSVP with IETF Integrated Services".

[20] IETF RFC 2401: "Security Architecture for the Internet Protocol".

[21] IETF RFC 2402: "IP Authentication Header".

[22] IETF RFC 2403: "The Use of HMAC-MD5-96 within ESP and AH".

[23] IETF RFC 2404: "The Use of HMAC-SHA-1-96 within ESP and AH".

[24] IETF RFC 2405: "The ESP DES-CBC Cipher Algorithm With Explicit IV".

[25] IETF RFC 2406: "IP Encapsulating Security Payload (ESP)".

[26] IETF RFC 3550: "RTP: A Transport Protocol for Real-Time Applications".

3 Abbreviations

For the purposes of the present document, the following abbreviations apply:

ACK	Acknowledge
AES	Advanced Encryption Standard
AH	Authentication Header
DARPA	Defence Advanced Research Projects Agency
DHCP	Dynamic Host Configuration Protocol
ESP	Encapsulating Security Payload
FIN	Finished
IANA	Internet Assigned Numbers Authority
ICMP	Internet Control Management Protocol
ICV	Integrity Check Value
IKE	Internet Key Exchange
IP	Internet Protocol
ISDN	Integrated Services Digital Network
ISO	International Standards Organisation
IV	Initialization Vector
MAC	Message Authentication Codes
NAT	Network Address Translation
OSI	Open Standards Interconnection
PSH	Push
QoS	Quality of Service
RH	Routing Header
RST	Reset
RTP	Real time Transport Protocol
SA	Security Association
SAP	Service Access Point
SCN	Switched Circuit Network
SHA	Secure Hashing Algorithm
SPI	Security Parameters Index
SYN	Synchronize
TCP	Transport Control Protocol
UDP	User Datagram Protocol
URG	Urgent

4 Security analysis of IPv6

4.1 Overview

The security analysis of IPv6 is performed against the core security attributes:

- Confidentiality.
- Integrity.
- Availability.

In addition the analysis of security provisions in a network using IPv6 is considered against the Framework Directive [6].

4.2 Confidentiality

Providers of ECN&S have a duty to ensure that communications are confidential. IPsec provides a mechanism for confidentiality of the payload of an IPv6 packet.

4.3 Integrity

The Framework Directive [6] addresses integrity in the context of network availability and not in terms of data manipulation. IPsec provides a mechanism for validating the integrity of the payload of an IPv6 packet.

4.4 Availability

Historically in the circuit switched era of communication availability has been a major goal of the network operator and there are rules established in the communications directives for availability which are often roughly translated as 5-nine reliability (i.e. the network has to be available 99,999 % of the time). This translates to a very small down time for the network overall (a little over 5 minutes down time per year). Availability has been maximized by using optical networks (reducing the potential for attacks on availability through electromagnetic interference), by using digital transmission (reducing attacks on availability through signal attenuation allowing differential bit recovery), by introducing some redundancy and by some over capacity engineering (to cope with maintenance of availability in the presence of exceptional offered traffic loads). In the packet era over an optical network the availability of core connectivity is theoretically the same as for the optical switched network. Where availability is compromised is in the addition of packet processing at each node and IP can be relatively processor heavy which reduces availability. Where the processor load is a variable dependent upon the content of the packet there is potential to reduce network availability by tailoring packets to maximize processor load in order to deny service to the next packet.

The second major change in the packet switched era is the availability of intelligent network elements outside the core of the network. In the traditional network the routing and signalling were under the control of the core network. In the IP era elements at the edge of the network may make routing and signalling commands. In many instances the inability of the core network to police traffic and signalling content has been elemental in the growth of security concerns in telecommunications.

IPv6 does not address availability.

NOTE: The transport protocols that may be used alongside IPv6 (TCP, UDP) address availability.

5 Internet protocols and OSI

5.1 Historical considerations

The International Standards Organisation (ISO) developed a model for communications protocol development and description in the mid 1970s, which is widely known as the Open Systems Interconnection model or more commonly by either its abbreviation OSI, or by the term the OSI stack, or by the term the OSI model. The OSI model was intended as a means to encourage manufacturers of communications devices (hardware and software) to have a single model with well defined interfaces and responsibilities within the stack and protocols across a communications path between corresponding layers for future development with a view to allow opening up of a new market in data communications.

The Internet Protocol, and its stack, was developed some years before the OSI model. There are a number of paths of development that were taken in the development of IP. For small mesh connected systems where individual nodes of the mesh are unreliable (i.e. not guaranteed to be available at all times) the routing protocol of IP will ensure that the transmitted packet arrives hence an unreliable network supports reliable transmission. IP is able to use any communications medium wherein IP acts as a virtual link layer when compared to OSI. What this means in effect is that a set of different technologies built using their own interpretation of the OSI model can be made to appear as a seamless data communications network by having an IP abstraction layer put on top. There are several technologies in the IP family that allow this but essentially the binding of an IP address to a technology specific address abstracts the technology specific address and specific network behaviour away from the applications that sit above IP.

Many early papers and books describing OSI talked of the "wine-glass" shape. What this meant was that a wide spectrum of applications (the rim of a wine glass) can be delivered over a wide spectrum of communications technologies (the base of the wine glass) by having only one transport protocol (the middle layer of the OSI model). What IP has offered to the data-communications industry is the narrow stem of the hypothetical wine glass.

The attraction of IP, as the idealised technology abstraction layer, to the data communications universe is well documented. Essentially it has allowed applications developers to adopt the mantra of "write once, deploy everywhere" and not worry about the binding of the technology specific OSI layers 1 to 4 to the IP model.

The beauty of IP is somewhat tarnished when the application requires knowledge of the real behaviour of the networks that IP is abstracting. Very simply IP does not report any real time knowledge of the network to the applications lying above it. This is a problem if one is using IP for voice -such as in telecommunications services.

The base IP protocol is absolutely fair in its approach to packet treatment. They are all treated the same. This is strength as well as a weakness. The greatest strength is that for many applications where data communications is required the application designer can be assured that the data will get through without error and will be reordered so the communicating applications receive what is transmitted. This is great for web browsing, e-mail, terminal emulation (the original killer-app of the Internet).

As IP is absolutely fair in its treatment of packets it cannot make full use of the technology that it is abstracting. This means, for example, establishing communications connections, restoring connections, optimizing the IP packet to the packet carrying capabilities of the underlying technology, recognizing and reporting errors in the underlying communications technology.

5.2 Seven layer OSI stack

The OSI model works by each layer providing a set of services to the upper layer accessible through a Service Access Point (SAP). In the ISDN model this allows a set of services such as "Call Setup" to be offered by one layer to another. Each layer communicates with its peer across the network with some layers having scope from end to end and some having scope of a link or a network.

The OSI security model generally uses key management at layer N+1 to protect data at layer N. In many instances (DECT, GSM, TETRA) this is achieved by authentication mechanisms at layer 3 providing a key for an encryption mechanism at layer 2.

5.3 Five layer IP stack

The IP stack is described by Tannenbaum [4] and others as a 5 layer stack.

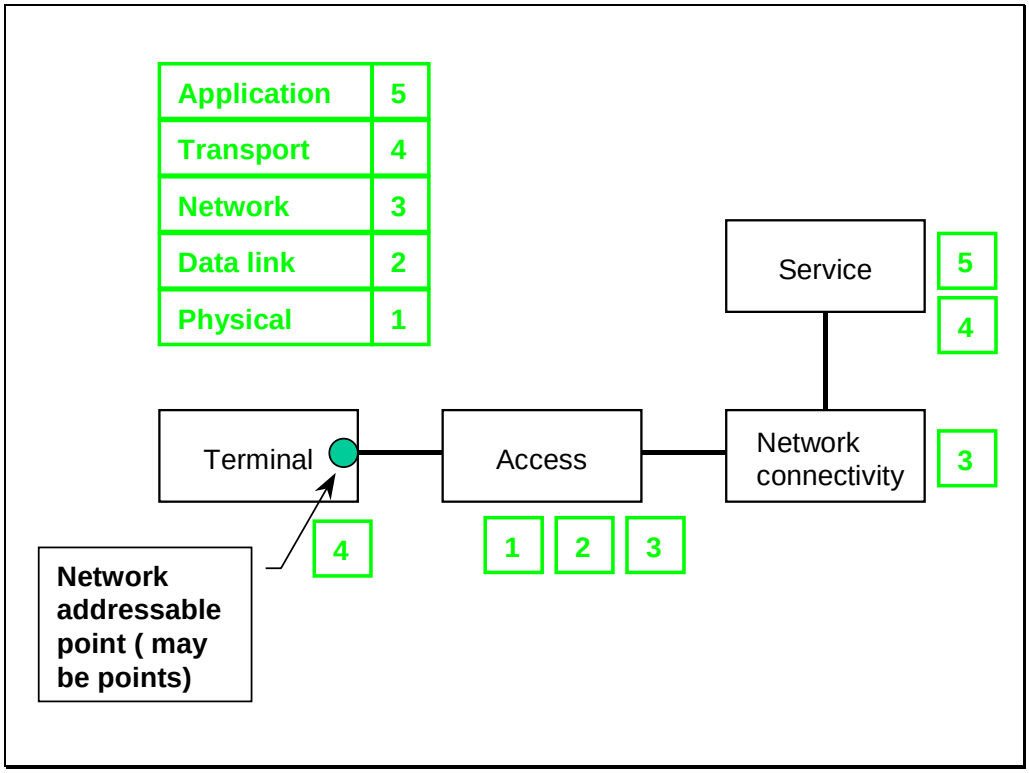


Figure 1: Basic data model for IP connections

Consider figure 1. The component parts are defined as in table 1, with additions below. The layers column shows which layers in the 5-layer IP model the component is active at.

Table 1: Active Components in the 5-Layer Model

Component	Definition	Layers
The terminal	Some apparatus, of arbitrary complexity, which is connected by the user to the access mechanism. The terminal, or elements of the terminal, is under the user's control. (The terminal may itself be a network of arbitrary complexity. The terminal possesses one or more **network addressable points** (IP address and port pair)).	1, 2, 3, 5
The access	A mechanism, provided by a party other than the user, which connects the terminal to some point which provides network connectivity. The access mechanism does not have the functionality to offer connectivity between one terminal and another, other than through the network connectivity mechanism.	1, 2, 3
Network connectivity	An arrangement of equipment which offers connectivity between one terminal and another.	3
The service	A set of functions offered to a user by an organization or a mechanism which offers functionality to another network component.	5

6 Summary of IPv6

6.1 Introduction

IPv6 is an extension and significant redesign of IPv4 although without notable change of scope. The original publication of IPv4 (dated September 1981) was drafted under the editorship of Jon Postel for the Defence Advanced Research Projects Agency (DARPA) of the United States of America Government, as a specific DARPA Internet Protocol. IPv6 edited under the leadership of Stephen Deering and Robert Hinden was pumped largely as a result of changes in application of IP and in particular the growth in the number of nodes and applications using IP and in particular the public Internet as an interconnection protocol.

6.2 Services in IPv6

There are a number of services associated with IPv6 and most are considered in terms of the Internet Control Message Protocol (ICMP).

6.2.1 Address allocation

The allocation of addresses in IPv6 is a major change from the methods adopted in IPv4 and by default all IPv6 nodes start by requesting address autoconfiguration.

Address space was, at one time, running out in the IPv4 based internet. A number of methods of address space management have been employed in IPv4 networks and include DHCP (Dynamic Host Configuration Protocol in which the address is granted temporarily to a host from a pool managed by the DHCP server) and NAT (Network Address Translation in which a large pool of private addresses are mapped to a small pool of public addresses).

The size of the address field in IPv6 suggests that address exhaustion is unlikely (there are less than 2 128 objects in the known universe). However there are concerns of privacy in making the address public or deducible which need further evaluation.

FOR FURTHER STUDY:
The security implications of address provision in IPv6 within the context of the Framework Directive have not been fully explored.

6.3 Protocol considerations

The classification of IPv6 as a protocol is often hard to justify as the behaviour is not rigorously stated. Most ISO protocols are described in the context of finite state machines whereas IPv6 does not have an explicit state machine and is often referred to as stateless. Notwithstanding this the essential behaviour of a node in an IPv6 network is to examine the destination address of the received packet, compare it with address of the node and then if the address is the same as that of the node to process the packet, else to pass the packet on. In this simplified view IPv6 does not differ from IPv4.

The IPv6 header is shown in table 2.

Table 2: IPv6 Header

Field name	Size (bits)	M/O/C	Function/comment
Version	4	M	6
Traffic class	8	M	Used to identify and distinguish between classes of packets.
Flow label	20	M	Experimental, used to label sequences of packets.
Payload length	16	M	Number of octets following the destination address.
Next header	8	M	This field makes use of the Protocol field values of the IPv4 header, and allows one to indicate the first of subsequent IPv6 extension headers (e.g. for authentication and encryption), IP in IP encapsulation, or an upper layer protocol.
Hop limit	8	M	Similar to the way time to live is used in IPv4, packet is discarded when this field is decremented to zero.
Source address	128	M	The address of the originator of the IPv6 packet.
Destination address	128	M	The address of the next network layer recipient of the IPv6 packet.
Number of bits	320		

6.4 Field by field comparison of IPv6 and IPv4

Comparing the IPv6 header (see table 2) to the IPv4 header (see table 3) the essential content is the same. The header checksum and three fields used for fragmentation have disappeared. IPv6 has a fixed length basic header with possible extension headers added, where intermediate nodes do not look at any point after the destination address with the exception of an IPv6 Hop-by-Hop Option extension header.

Table 3: IPv4 Header

Field name	Size (bits)	M/O/C	Function/comment
Version	4	M	4
Internet Header Length	4	M	Minimum value is 5 words (32 bits per word).
Type of service	8	M	Intended for use in QoS. Not consistently applied.
Total length	16	M	Of datagram including header.
Identification	16	M	
Flags	3	M	Used to control fragmentation.
Fragment offset	13	M	
Time to live	8	M	
Protocol	8	M	As identified in STD002.
Header checksum	16	M	Recomputed at every node (processing point of header).
Source address	32	M	
Destination address	32	M	
Options	24	O	Optional to be transmitted. Capability has to exist.
Padding	8	O	Ensures that header ends on a 32-bit boundary.
Number of bits (minimum)	160		

Table 4: Field by field comparison of IPv6 and IPv4 Headers

IPv6 Field name	IPv6 Size (bits)	IPv4 Size (bits)	Comment
Version	4	4	Incremented from 4 to 6.
Traffic class	8	n/a	
Flow label	20	n/a	Approximately equivalent to Type of Service field in IPv4.
Payload length	16	16	
Next header	8	n/a	Equivalent to the "Protocol" field in IPv4.
Hop limit	8	n/a	Equivalent to the "Time to live" field in IPv4.
Source address	128	32	Hugely increased by 2^{96} times.
Destination address	128	32	Hugely increased by 2^{96} times.

6.5 Options and their use in IPv6

A summary of how to use options is described here with respect to RFC 2460 [7].

Table 5: IPv6 Packet construction

Field name	Size (bits)	M/O/C	Function/comment
IPv6 Header	320	M	
Hop-by-hop options header			
Destination options header (*every* Routing Header destination)			
Routing header			
Fragment header			
Authentication header	96 + 32n		
Encapsulating Security Payload header	96 minimum		
Destination options header (*last* Routing Header destination)			
Upper-layer header			May be another IPv6 header and extensions.

The first octet of each of the extension headers is a "Next header" field.

The use of extension headers and the "Next header" field is shown better diagrammatically below:

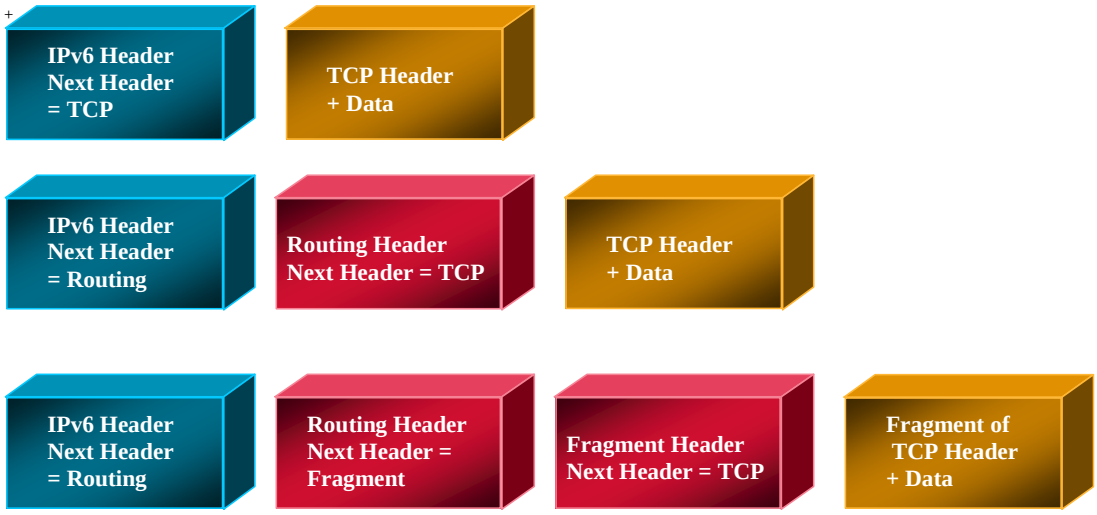


Figure 2: IPv6 header chaining

6.6 TCP, RTP and UDP

IPv6 as shown in figure 2 does not work standalone but operates within a layered protocol stack. Most commonly the data being carried is one of four types: connection oriented non-real time data carried using the Transmission Control Protocol (TCP, defined in RFC 793 [8]); connectionless data carried using User Datagram Protocol (UDP, defined in RFC 768 [9]); real time connection oriented data carried using the Real Time Streaming Protocol (RTSP, defined in RFC 2326 [10]); or, more commonly the real-time transport protocol (RTP a protocol for real-time applications defined in RFC 1889 [11]).

For example, how do the differences between IPv4 and IPv6 impact these ULPs? What security mechanisms exist for each above IP and IPsec? What are the ramifications of using IPsec versus higher layer security. For example, a policy of using AH or ESP can provide some protection to TCP (sequence number guessing, port scanning, SYN flooding, forged RSTs, hijacking), whereas TLS or SSH is useless against the first four of these five. But IPsec may be a bigger problem for firewalls. IPv4 is more likely, perhaps, to use NAT, and IPv6 may be more friendly to end-to-end IPsec.

6.6.1 TCP header and its use (from RFC 793)

SECURITY IMPACT: Availability and Integrity

Transmission Control Protocol (TCP) provides a reliable and continual data flow between two endpoints on the network. It provides a full duplex service to the application layer, which means that data can flow in both directions. For an application it is similar to a byte stream. The data is sent into the stream assuming that it will arrive at the other end, byte after byte, in the correct order. However, IP neither guarantees packet delivery nor an arrival of data packets only once and in the right order. Therefore, TCP must have its own mechanism.

NOTE: Whereas IP is nominally stateless the use of TCP makes the connection and connection maintenance stateful.

Every TCP packet has a sequence number that allows the recognition of missing packets, packets received in the wrong order or duplicated packets. TCP splits the data intended to be sent into best sized "chunks". This unit of information is called a segment. For every received segment, an acknowledgement is sent back to the sender. This confirms the reception of the packet. If the packet does not arrive in a certain time interval (the sender does not receive an acknowledgement), the sender retransmits the packet. If packets arrive out of order, they can be reassembled because of the sequence numbers in each TCP packet. The technique that ensures the reliable transmission of data is called sliding window.

The header fields needed for this functionality and all the others are illustrated in table 6.

Table 6: TCP header

Field	Size	M/O/C	Function/comment
Source port	16	M	Port number of the process sending data Well, OK, but not exactly. The four-tuple of addresses and ports identify the process on each end.
Destination port	16	M	Port number of the process receiving data.
Sequence number	32	M	Offset number of the first data byte of the payload in the byte stream.
Acknowledgement number	32	M	Points to the sequence number of the octet following received and read data.
Data offset	4	M	Defines the offset of the data in this TCP segment.
Reserved	6	M	Reserved for future use. Must be zero.
Flags	6	M	Six flags.
Window	16	M	Used for the advertisement of the transmission window size.
Checksum	16	M	Is calculated over TCP header and payload.
Urgent pointer	16	M	Points to the sequence number of the octet following the urgent data.
Options	1 to 32	O	Variable.
Padding	0 to 32	O	For maintaining a multiple of 32.
Number of bits	160 minimum		

The flags field contains six flags:

- Urgent (URG): It enables urgent mode. One end signals the other end that some form of urgent data has been placed into the stream.
- Acknowledge (ACK): It indicates that the acknowledgement number contained in this TCP packet is valid.
- Push (PSH): It asks the receiver to pass the data to the application as soon as possible.
- Reset (RST): It resets the connection.
- Synchronize (SYN): It is used during the connection establishment to synchronize sequence numbers.
- Finished (FIN): Its sender indicates that it wants to terminate the connection.

6.6.1.1 Reliability

Reliability is one the *raison d'etre* of the Transmission Control Protocol. Generally called a reliable protocol TCP will always get the data through. It does so without regard, generally, to delay or to throughput. If a packet is lost the packet transmission rate is dropped and the missing packet retransmitted. As the success rate increases so does the packet rate.

6.6.2 UDP header and its use (from RFC 768)

SECURITY IMPACT: Availability

User datagram protocol (UDP) is another transport protocol that uses IP for its service. It resides in the transport layer [4] of the layered IP stack model of section 4.3. The purpose of UDP is to provide a multiplexed a datagram service between two hosts. This means that individual datagrams, chunks of data, may be sent from one host to the other and delivered to the correct process on each end. The UDP header introduces two fields for addressing the ports of the processes that interact. The source-port field and the destination-port field. Important properties of UDP are that there are no mechanisms to guarantee the delivery of a packet or to detect duplicate packets. The datagram service of UDP is therefore also referred to as being an "unreliable service".

The fields of the UDP header are listed in table 7:

Table 7: UDP header

Field name	Size	Function/comment
Source port	16	Port number of the process sending the datagram.
Destination port	16	Port number of the process receiving the datagram.
Length	16	Length of the UDP header and data.
Checksum	16	Checksum over UDP header and data.
Number of bits	64	

6.6.2.1 Reliability

UDP is unreliable and any packet lost by UDP remains lost and UDP makes no attempt to recover.

6.6.3 RTP header and its use (from RFC 1889 superseded by RFC 3550)

SECURITY IMPACT: Availability and Integrity

This protocol supports end-to-end delivery of data with real-time characteristics, such as video or audio. It is the basis for VoIP telephony protocols. For example SIP and H.323 use it to deliver voice data.

To fulfil its purpose RTP uses the services of the transport layer protocol, which is in most cases UDP. UDP does not have integrated mechanisms to reorder packets or retransmit lost ones, and RTP does not have them either. But RTP allows applications to reassemble the RTP packets. The fields enabling it are sequence number and timestamp in the RTP header.

RTP actually consists of two parts. The first, RTP itself, carries the data with real-time properties. The second one is RTCP, which is a lightweight session control protocol to monitor quality of service (QoS). RTP and RTCP use consecutive transport layer ports when running on UDP. Moreover, RTP defines for each class of application one profile and one or more formats. A profile is information for the application to understand the meaning of certain fields of the RTP header. The format describes how the data sent must be interpreted. RTP leaves many protocol details to the specification of the profile and the format. This was a design issue from the beginning.

The header of RTP is shown in table 8:

Table 8: RTP header

Field name	Size	M/O/C	Function/comment
Version	2	M	Version.
Padding bit	1	M	Padding bit.
Extension bit	1	M	Extension bit.
CC	4	M	Number of contributing sources.
Marker	1	M	Marker bit.
Payload Type	7	M	Payload type.
Sequence number	16	M	Number to identify the RTP packet in a stream.
Timestamp	32	M	Sampling time of the first byte of the payload.
Synchronization source identifier	32	M	Identifies the source of the data.
Contributing source identifier(s)	32	O	Identifies the contributing sources for the payload.
Number of bits	96 (minimum)		

RTCP is used to send control information to all participants of a session. The information is sent on a periodic basis. A separate connection (pair of ports) is used to deliver the control data. The transport protocol is UDP, as in RTP.

RTCP implements four functions: Firstly, it has to deliver information about the quality of the data distribution. It secondly supplies a persistent transport-level identifier for every participant. This functionality permits for instance the indication of the source of the stream. The third function is the possibility of calculating the number of participating parties. This is accomplished by sending the control information to every other participating party. The fourth and last functionality is the support of a minimum session control.

RTCP defines several different packet types:

- SR is a sender report and conveys statistical data of an active sender.
- RR is a report of a receiver for statistics of a participant that does not actively send data.
- SDES contains source description items.
- BYE indicates the end of a participation.
- APP consists of application specific data.

The packet format starts with a fixed pattern. It is followed by structured elements of variable length. The packet has an aligned boundary of 32 bits. This allows the concatenation of several RTCP packets to one compound packet. These cumulative packets are sent in one UDP datagram.

6.6.3.1 Reliability

As RTP uses UDP, and as UDP is unreliable, then RTP is unreliable.

7 Quality and grade of service

SECURITY IMPACT: Availability

QoS-related specifications of the IETF often refer to both IPv4 and IPv6. Examples:

- DiffServ: RFCs 2474, 2475
- RSVP: RFCs 2205-2210

The IPv6 header has two QoS-related fields:

- 20-bit Flow Label which may be used by a source to label sequences of packets for which it requests special handling by IPv6 routers. This label is geared to IntServ and RSVP.
- 8-bit Traffic Class Indicator which may be used by originating nodes and/or forwarding routers to identify and distinguish between different classes or priorities of IPv6 packets. This is geared to Diffserv.

If we look at the IPv6 packet structure we see a large header field (constant length of 320 bits), followed by a variable number of extension headers, and a variable length payload. If we were to assume (for the sake of illustration) that we wished to transport 20 ms of speech per packet where the speech is originally encoded using the G.711 model (i.e. 64 kb/s, or 8-bit samples every 125 μs) then each speech sample would contain 1 280 bits to go into the payload. We would ideally encode this using RTP and add an RTP header. So we will end up with approximately 40 % of overhead in the transmission path.

8 Security in IPv6

8.1 Overview

IPsec is the security architecture for the Internet Protocol (IP). The architecture is designed to enable provision of the following security services at the IP layer: access control, connectionless integrity, data origin authentication, protection against replay attacks, confidentiality, and limited traffic flow confidentiality. IPsec is applicable to both IPv4 and IPv6.

The architecture is defined in RFC 2401 [20] and addresses the following 4 elements:

- *Security Protocols*: Authentication Header (AH) (RFC 2402 [21]) and Encapsulating Security Payload (ESP) (RFC 2406 [25]).
- *Security Associations*: Definition, management and processing.
- *Key Management*: The Internet Key Exchange (IKE).
- *Algorithms*: Requirements of the authentication and encryption algorithms.

NOTE: The IPsec protocol suite does not define the authentication and encryption algorithms used in implementations. These are defined in individual RFCs per algorithm.

In general, IPsec-related specifications (see e.g. RFCs 2401-2406) are specified for both IPv4 and IPv6. The basic difference is that the support of basic IPsec functions is mandatory in IPv6, while they are optional in IPv4, and are not supported by many IPv4 implementations within the current Internet.

IPsec is a policy enabled architecture and the policy is pointed to by the protocols using a Security Association (SA) identified by the triplet of " Security Parameters Index, destination IP addresses, type of protocol header (AH or ESP)". The management and allocation of SAs has been standardized many times and the Internet Key Exchange (IKE) is noted as the default in RFC 2401 [20]. This does not suggest that IKE is the only automated key management scheme to be used in IPsec and many applications use alternative approaches.

8.2 Security protocols

8.2.1 Overview

Traffic security is provided by two security protocols (in addition to the Architecture [RFC 2401 [20], which is an integral part of the security):

- The Authentication Header protocol (RFC 2402 [21]); and,
- Encapsulating Security Payload protocol (RFC 2406 [25]).

Either of these protocols may be applied alone or in combination, to provide the desired level of security. The IPSec security protocols are represented by headers that appear before the IP header in the IP packet.

8.2.2 Authentication Header (from RFC 2402)

The *Authentication Header* protocol provides connectionless integrity and data origin authentication. There is also an optional anti-replay service available.

The AH protocol provides a cryptographic digest of the data being transmitted. Assuming that the Security Association for the end-points in communication is sound then the checking of the digest will provide both authentication of the transmitter, and check the integrity of the data transmitted.

Table 9: AH contents

Field name	Size (bits)	M/O/C	Function/comment
Next header	8	M	As per IPv6 header.
Payload length	8	M	Specifies the length of AH in 32-bit words (4-byte units), minus "2."
Reserved	16	M	Reserved for future use, default value is "zero".
Security Parameters Index (SPI)	32	M	Used to uniquely identify the Security Association of the current datagram in combination with the destination IP address and the security protocol. (In 2401 bis, SPI and destination address alone suffice.)
Sequence number field	32	M	Used for replay protection.
Authentication data	N times 32	M	Contains the Integrity Check Value (ICV) for this packet.
Number of bits	96+(32N)		

8.2.2.1 Authentication Algorithms

The authentication algorithm employed for the ICV computation is specified by the Security Association (SA). For point-to-point communication, suitable authentication algorithms include keyed Message Authentication Codes (MACs) based on symmetric encryption algorithms (e.g. DES, AES) or on the HMAC construction with one-way hash functions (e.g. MD5 or SHA-1). For multicast communication, one-way hash algorithms combined with asymmetric signature algorithms are appropriate, though performance and space considerations may preclude use of such algorithms. The mandatory-to-implement authentication algorithms are HMAC with MD5, and HMAC with SHA-1. Other algorithms may be supported.

8.2.2.2 Scope of ICV computation

The AH ICV is computed over:

- IP header fields that are either immutable in transit or that are predictable in value upon arrival at the endpoint for the AH SA;
- the AH header (Next Header, Payload Length, Reserved, SPI, Sequence Number, and the Authentication Data (which is set to zero for this computation), and explicit padding bytes (if any));
- the upper level protocol data, which is assumed to be immutable in transit.

If a field may be modified during transit (i.e. is mutable), the value of the field is set to zero for purposes of the ICV computation. If a field is mutable, but its value at the (IPsec) receiver is predictable, then the predictable value is inserted into the field for purposes of the ICV calculation (for example the destination address is mutable but predictable when using routing header extensions).

Table 10: Scope of AH mechanisms (in IPv6) in transport mode

IP Header	Ext header	AH header	TCP	Data
Authenticated except for mutable fields				

Table 11: Scope of ESP mechanisms (in IPv6) in tunnel mode

New IP Header	New ext. headers	AH header	Original IP header	Original ext. headers	TCP	Data
Authenticated except for mutable fields in new headers						

Tables 10 and 11 indicate the scope of the authentication and integrity check. Replay protection is provided by use of the sequence number field and allows 232 IP packets to be transmitted during the lifetime of the SA. Alternatively the lifetime of an SA where replay protection is used is restricted to 232 IP packets.

8.2.3 Encapsulating Security Payload (from RFC 2406)

The *Encapsulating Security Payload* protocol potentially provides two types of security service. The first being confidentiality via encryption and limited traffic flow confidentiality. The second type is connectionless integrity, data origin authentication and an anti-replay service. (It can do either or both, but it MUST NOT do neither.)

Table 12: ESP contents

Field name	Size (bits)	M/O/C	Function/comment
Security Parameters Index (SPI)	32	M	Used to uniquely identify the Security Association of the current datagram in combination with the destination IP address and the security protocol.
Sequence number field	32	M	Used for replay protection.
Payload data	Variable	M	
Padding field	0 to 2048		
Pad length	8	M	
Next header	8	M	
Authentication data	N times 32	O	Contains the Integrity Check Value (ICV) for this packet.
Number of bits	96 minimum		
NOTE 1: The SPI and Sequence number fields constitute the header of ESP, the pad length and next header field constitute the tail of ESP. NOTE 2: The payload data plus padding field plus Pad length plus Next header are encrypted.			

Table 13: Scope of ESP mechanisms (in IPv6) in transport mode

IP Header	Ext header	ESP header	ESP payload (payload data plus padding fields)			ESP trailer	ESP authentication
			Destination option headers	TCP header	Payload (data being protected)		
			Encrypted				
		Authenticated					

Table 14: Scope of ESP mechanisms (in IPv6) in tunnel mode

New IP Header	New ext. headers	ESP header	ESP Payload (payload data plus padding fields)				ESP trailer	ESP auth
			Original IP Header	Original ext. headers	TCP header	Payload (data being protected)		
			Encrypted					
		Authenticated						

8.2.3.1 Encryption Algorithms

The encryption algorithm employed is specified by the SA. ESP is designed for use with symmetric encryption algorithms. Because IP packets may arrive out of order, each packet must carry any data required to allow the receiver to establish cryptographic synchronization for decryption. This data may be carried explicitly in the payload field, e.g. as an IV (as described above), or the data may be derived from the packet header. Since ESP makes provision for padding of the plaintext, encryption algorithms employed with ESP may exhibit either block or stream mode characteristics. Padding may also be used for obscuring traffic characteristics.

NOTE 1: Since encryption (confidentiality) is optional, this algorithm may be "NULL".

A compliant ESP implementation shall support the following algorithms:

- DES in CBC mode (for confidentiality);

NOTE 2: DES has largely been deprecated in practice and instead use of 3DES and AES are accepted practice.

- HMAC with MD5 (for authentication);
- HMAC with SHA-1 (for authentication);
- NULL Authentication algorithm;
- NULL Encryption algorithm.

Since ESP encryption and authentication are optional, support for the 2 "NULL" algorithms is required to maintain consistency with the way these services are negotiated. However while authentication and encryption can each be "NULL", they shall not both be "NULL".

8.2.3.2 Authentication Algorithms

The authentication algorithm employed for the ICV computation is specified by the SA. For point-to-point communication, suitable authentication algorithms include keyed Message Authentication Codes (MACs) based on symmetric encryption algorithms (e.g. DES) or on one-way hash functions (e.g. MD5 or SHA-1). For multicast communication, one-way hash algorithms combined with asymmetric signature algorithms are appropriate.

NOTE: Since authentication is optional, this algorithm may be "NULL".

8.2.4 Comparison of AH and ESP

ESP tunnel mode can provide the same level of protection as AH, when authentication is used. However, when ESP is used in transport mode, the IP Header remains unprotected because only the packet payload is secured. AH provides protection of IP header as far as this is possible. However, as some IP header fields may change in transit, the values of these fields cannot be protected by AH.

8.3 Security associations

The AH and ESP headers do not contain information pertaining to the cryptographic algorithms and their associated parameters. These representations are achieved through the transmission of a *Security Parameters Index* (SPI). This index combined with the destination IP addresses and the type of protocol header (AH or ESP) determines the parameters of the IPsec processing.

These parameters of a unidirectional security service are represented by a *Security Association* (SA). There are two types of AH or ESP SAs:

- *Transport Mode SA:* This is a security association between two hosts, generally used to secure the traffic of the upper layer protocols.
- *Tunnel Mode SA:* This is a security association in an IP-in-IP tunnel, generally used in connecting to security gateways.

In the interdomain environment, enforcement of regional IPsec policies can create conflicts and result in problems for end-to-end communication. Standardization and inter-domain policy management will help ensure correct end-to-end protection and transmission.

8.3.1 Security Associations and Management

A Security Association (SA) is a relationship between two or more entities that describes how the entities will utilize security services to communicate securely. This relationship is represented by a set of information that can be considered a contract between the entities. The information must be agreed upon and shared between or among all the entities. Sometimes the information alone is referred to as an SA, but this is just a physical instantiation of the existing relationship. The existence of this relationship, represented by the information, is what provides the agreed upon security information needed by entities to securely interoperate. All entities must adhere to the SA for secure communications to be possible.

The SA attributes required and recommended for the IP Security (AH, ESP) are defined in RFC 2401 [20], section 4. The attributes specified for an IP Security SA include, but are not limited to, authentication mechanism, cryptographic algorithm, algorithm mode, key, key length, Lifetime, and Initialization Vector (IV). IV may depend on some seed or state. Other protocols that provide algorithm and mechanism independent security MUST define their requirements for SA attributes. The separation of IKE from a specific SA definition is important to ensure IKE can establish SAs for all possible security protocols and applications.

In order to facilitate easy identification of specific attributes (e.g. a specific encryption algorithm) among different network entities the attributes must be assigned identifiers and these identifiers must be registered by a central authority. The Internet Assigned Numbers Authority (IANA) provides this function for the Internet.

Private algorithms, however, are allowed.

8.4 Key Management

IPsec mandates support for two separate methods of cryptographic key and SA management:

- *Manual Key Management:* This is the simplest form of key management and involves each IPsec connection to be configured manually on both hosts. While this maybe suitable in small static situations, it is unsuitable in larger deployment scenarios due to scalability problems.
- *Automatic Key and SA Management:* Larger deployment scenarios call for an Internet-standard, scalable and automated SA and key management protocol. This is provided by *Internet Key Exchange* (IKE). IKE is a hybrid protocol, using the ISAKMP "phases" and OAKLEY "modes". (It also includes pieces of Photuris and SKEME.) IKE is required to allow for use of anti-replay features of AH and ESP and to facilitate on-demand creation of SAs.

It is expected that many systems choosing to implement ISAKMP will strive to provide a protected domain of execution for a combined IKE key management daemon.

9 Architecture and protocol implications

When specifying IPv6, the IETF was keen to keep the amount of changes to the existing (IPv4-based) Internet architecture and to the set of services supported very low. Correspondingly, IPv6 by itself is not expected to require major architectural changes to basic TIPHON specifications.

Although IPv6 by itself would not imply any major architectural changes it has to be recognized that there may be a transition phase to IPv6, where IPv4 and IPv6 networks co-exist in parallel for many years. This implies that an end-to-end communication may involve scenarios such as SCN - IPv4 - IPv6 or SCN - IPv6 - IPv4 . Additional devices for IPv6-over-IPv4 tunnelling, or for IPv4-IPv6 address translation may have an impact on the provision of end-to-end voice services. It should also be noted that the co-existence of IPv4 and IPv6 may have an impact on routing decisions (e.g. related to the selection of a gateway).

Currently, no specific "IPv6-Applications" are envisaged. Applications which do not make direct use of IP addresses, are expected to run over IPv4 in the same way as over IPv6. For those IPv4-applications which make direct use of IP addresses (e.g. DNS, DHCP, Routing protocols), adaptations to IPv6 have been, or are in the process of being, specified. A possible address translation by gateways or tunnelling devices between IPv4 and IPv6 may, however, have an impact on end-to-end communications where a separate control information flow is used which refers to IP addresses used in a related flow of packets (e.g. for voice communication).

9.1 Security associations and key management

The IPsec ESP mode of operation, tunnel mode versus transport mode, has a significant impact on the key management domain. Note that this is essentially a "hop by hop" versus "end-to-end" question rather than tunnel mode versus transport mode. Tunnel mode can be used anywhere. This is not just a performance or overhead question. It is also a security and functionality issue.

Each SA is defined by the unique combination of SPI and Destination address. The impact of this is shown in figure 3 which shows an example of two users A and B communicating across a network consisting of 4 nodes (1, 2, 3, 4). The normal routing model suggests the following routes are available to any packet from A to B:1-4; 1-2-4; 1-2-3-4; 1-3-2-4; 1-2-4; 1-3-4. In a transport mode implementation employing IPsec each node has to have an SA for each node it connects to. In tunnel mode only one association is required for the communication from A to B. In the transport option each node has to have N-1 SAs (where N is the number of nodes it is connected to).

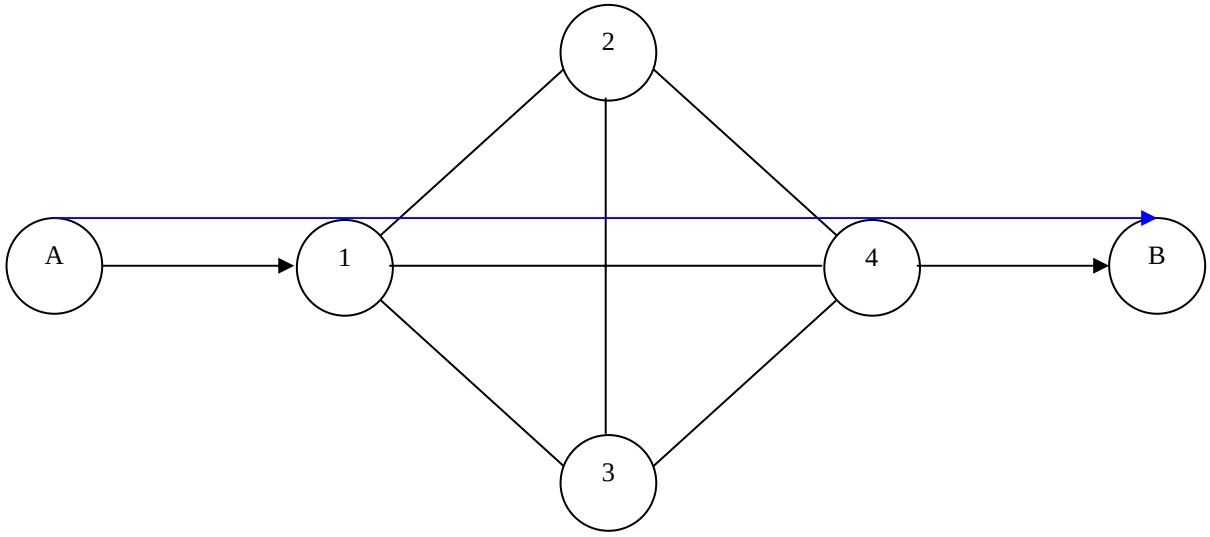


Figure 3: Transport mode versus tunnel mode links (A communicating with B)

10 Material for further study

The main body of the present document identifies some areas where IPsec may provide some security capabilities in the NGN. However further work is required and this clause identifies specific items for future study.

10.1 Security association design

Any application of IPsec has to start from the design of the security associations. In designing the security association parameters the IPsec mode (AH or ESP, transport or tunnel mode), algorithm selection and members of the association are determined.

Choosing between tunnel and transport modes has to take into account the size of the infrastructure over which communication takes place and generally where the infrastructure is unknown (number of nodes, route of each packet, MTU) then transport mode is much more difficult to apply.

For tunnel mode, such as that used in VPNs, the end points are generally finite in number and communication tends to be many to one (e.g. a corporate LAN allowing remote access) in which case the SA can be fairly tightly controlled.

In a telephony application such as the PSTN with many millions of users making arbitrary connections to each other so that the security association of tunnel mode would be difficult and probably infeasible unless the SA declared all destination addresses using port X (noting that port number is not generally used in the SA) share a common SA (algorithm, IV structure, etc.).

The application sitting on top of IP does not, in general, know the SA to adopt as the IP address is not visible. However, SSL works.

10.2 Protocol and services

The IETF is still working on IPv6 security for ICMPv6, IPv6 firewalls, mobility, transition, etc., and IPsec and IKE are being revised.

Increased use of IPsec depends in a large part on PKI and API issues.

The "standard bag of tricks" for IPv6 firewalls has not been invented yet. Management tools, DNS, and intrusion detection will need to catch up too.

History

Document history		
V1.1.1	April 2005	Publication