WORLD METEOROLOGICAL ORGANIZATION
_____

COMMISSION FOR BASIC SYSTEM
OPAG ON
INFORMATION SYSTEMS & SERVICES

Expert Team on Enhanced Use of Data Communication Systems

Montreal, Canada, 27-31 May 2002

ISS/ET-EUDCS 2002/Doc. X
(20.V.2002 – Version 1.0)
_____

ITEM 4.3

ENGLISH only

RECOMMENDED PROCEDURES FOR INTERNET-BASED CONNECTIONS BETWEEN RTHS AND NMCS (VPN, IPSEC)

Submitted by Rémy Giraud – Invited Consultant

Summary and Purpose of Document

After giving various technical details on VPN and especially on IPSec this document suggest a practical solution usable to complement the GTS with secure connection over the Internet

ACTION PROPOSED

The session is invited to review the information on the document.

TABLE OF CONTENT

1 Introduction

After describing various concepts related to VPN and IPSEC, this document presents a potential methodology to introduce the technical solution on the GTS and presents why these tools can enhance communication capabilities among members for operational traffic exchanges.

Chapter 2 introduces the concept of VPN and presents various technical alternatives to IPSEC. As IPSEC is the most appropriate protocol for secure network-to-network communication the document will then focus on this solution.

Chapter 3 briefly describes what is IPSEC. IPSEC is not a simple solution to understand. It covers a lot of technical aspects, allows various flavors of algorithms, and is better describe as a framework instead of a protocol.

Chapter 4 focuses on application of IPSEC on the GTS. A tentative selection of protocols is proposed. It shows what benefits WMO members could expect from the use of IPSEC. It also shows the drawbacks of self-operated IPSEC VPNs

Chapter 5 shows the technical evolution of IP services from the operators. Evolving from Frame Relay to IP solutions operators offer VPN solutions either MPLS based or IPSEC based.

Chapter 6 give :

- a complete configuration example on Cisco routers with the protocols selected in chapter 3.
- a glossary of terms related to VPN

2 What is a VPN ?

2.1 Definition

The definition below come from **[1]**.

Perhaps the simplest method of attempting to arrive at a simple definition for VPN's is to look at each word in the acronym individually, and then subsequently tie each of them together in a simple, common sense, and meaningful fashion.

Let's start by examining the word **"network**" This is perhaps the least difficult term for us to define and understand, since the commonly accepted definition is fairly uncontroversial and generally accepted throughout the industry. A network consists of any number of devices which can communicate through some arbitrary method. Devices of this nature include computers, printers, routers, and so forth, and may reside in geographically diverse locations. The methods in which they may communicate are numerous, since there are countless electronic signaling specifications, and data-link, transport, and application layer protocols. For the purposes of simplicity, let's just agree that a "network" is a collection of devices that can communicate in some fashion, and can successfully transmit and receive data amongst themselves.

The term "**private**" is fairly straightforward, and is intricately related to the concept of "virtualization" insofar as VPN's are concerned, as we'll discuss in a moment. In the simplest of definitions, "private" means that communications between two (or more) devices is, in some fashion, secret – that the devices which are not participating in the "private" nature of communications are not privy to the communicated content, and that they are indeed completely unaware of the private relationship altogether. Accordingly, data privacy and security (data integrity) are also important aspects of a VPN which need to taken into consideration when considering any particular VPN implementation.
Another means of expressing this definition of "private" is through its antonym, "public." A "public" facility is one which is openly accessible, and is managed within the terms and constraints of a common public resource, often via a public administrative entity. By contrast, a "private" facility is one where access is restricted to a defined set of entities, and third parties cannot gain access. Typically, the private resource is managed by the entities who have exclusive right of access. Examples of this type of private network can be found in any organizational network which is not connected to the Internet, or to any other external organizational network, for that matter. With this definition the current GTS is a *private* network

These networks are private due to the fact that there is no external connectivity, and thus no external network communications. Another important aspect of "privacy" in a VPN is through its technical definition, as describing the privacy of addressing and routing system, meaning that the addressing used within a VPN community of interest is separate and discrete from that of the underlying shared network, and from that of other VPN communities. The same holds true for the routing system used within the VPN and that of the underlying shared network. The routing and addressing scheme within a VPN should, for all intents and purposes, be self-contained, but this degenerates into a philosophical discussion on the context of the term "VPN."
"**Virtual**" is a concept that is slightly more complicated. The New Hacker's Dictionary **[2]** defines virtual as –
virtual /adj./ [via the technical term "virtual memory", prob. from the term "virtual image" in optics] 1. Common alternative to {logical}; often used to refer to the artificial objects (like addressable virtual memory larger than physical memory) simulated by a computer system as a convenient way to manage access to shared resources. 2. Simulated; performing the functions of something that isn't really there. An imaginative child's doll may be a virtual playmate. Oppose {real}.
Insofar as VPN's are concerned, the definition in **2.** above is perhaps the most appropriate comparison for virtual networks. The "virtualization" aspect is one that is similar to what we briefly described above as "private," however, the scenario is slightly modified – the private communication is now conducted across a network infrastructure that is shared by more than a single organization. Thus, the private resource is actually constructed by using the foundation of a logical partitioning of some underlying common shared resource, rather than by using a foundation of discrete and dedicated physical circuits and communications services. Accordingly, the "private" network has no corresponding "private" physical communications system. Instead, the "private" network is a virtual creation which has no physical counterpart. The virtual communications between two (or more) devices is due to the fact that the devices which are not participating in the virtual communications are not privy to the content of the data, and that they are also altogether unaware of the private relationship between the virtual peers. The shared network infrastructure could, for example, be the global Inter-

net and the number of organizations or other users not participating in the virtual network may literally number into the thousands, hundreds of thousands, or millions.

A VPN can also said to be a **discrete** network **[3]** –
discrete \dis*crete"\, a. [L. discretus, p. p. of discernere. See Discreet.] 1. Separate; distinct; disjunct.
The discrete nature of VPN's allow both privacy and virtualization. While VPN's are not completely separate, per se, the distinction is that they operate in a discrete fashion across a shared infrastructure, providing exclusive communications environments which do not share any points of interconnection.
The combination of these terms produces **VPN** – a **private network** , where the privacy is introduced by some method of **virtualizatio**n. A VPN could be built between two end-systems or between two organizations, between several end-systems within a single organization or between multiple organizations across the global Internet, between individual applications, or any combination of the above.

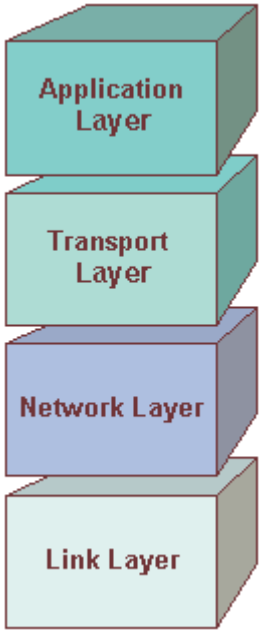
The common and somewhat formal characterization of the VPN, and perhaps the most straightforward and strict definition, is:

> **A VPN is a communications environment in which access is controlled to permit peer connections only within a defined community of interest, and is constructed though some form of partitioning of a common underlying communications medium, where this underlying communications medium provides services to the network on a non-exclusive basis.**

This definition introduces a concept, the VPN, not related to any technical implementation.

There are quite a lot of technical implementations of VPNs…

2.2 Types of VPNs



A simplified version of the TCP/IP layer model is shown on left.
The technical implementation of the VPNs are related to this model :

- On the link layer one can find :
  - ATM and Frame Relay connection
  - MPLS (Multi Protocol Label Switching)
  - Link-Layer Encryption (L2TP or PPTP)
- On the network layer :
  - IPSEC
- On the transport and application layer
  - SSL (Secure Socket Layer) is a protocol proposed by Netscape mainly for http traffic encryption
  - TSL (Transport Secure Layer) is a proposed standard by IETF (Internet Engineering Task Force) based on SSL
  - SOCKS
  - SSH

2.2.1 The Link Layer solutions

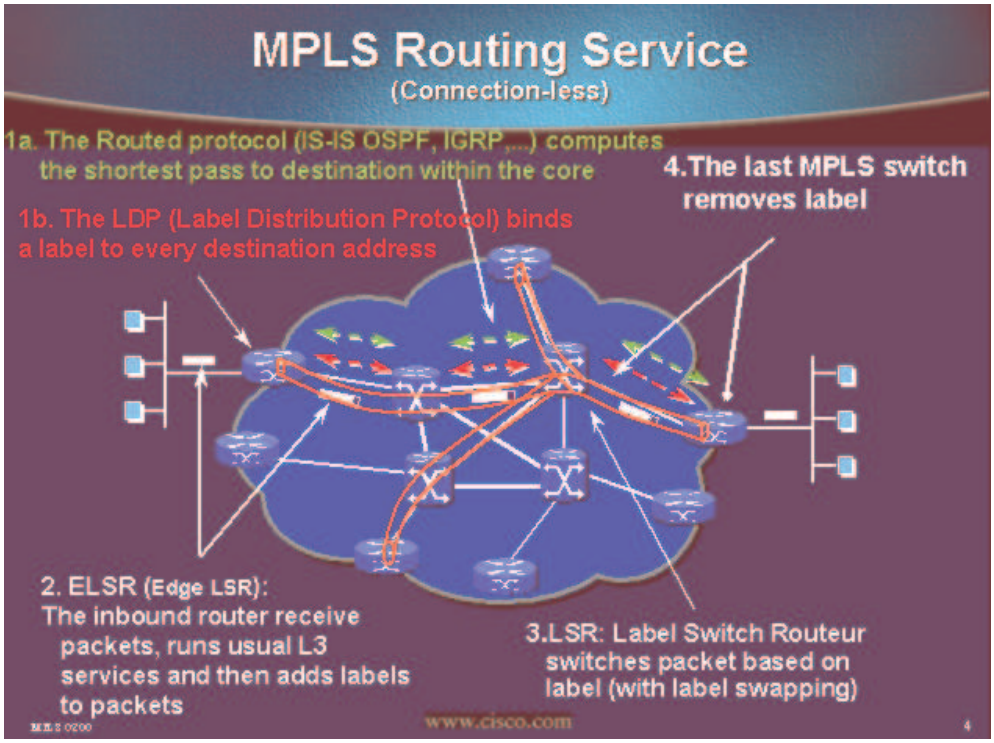
2.2.1.1 ATM and Frame Relay

Following the definition of VPNs gave on 1. ATM and Frame Relay solution must be considered as VPNs. By construction a Frame Relay (and ATM) network, like the RMDCN is a VPNs. The telco Equant has a network, which is securely

divided among all the customers. Therefore, on a global telecommunication system, coexist multiple isolated “sub-“networks. In this case, the VPNs rely on the operator.

2.2.1.2 MPLS

Nowadays, as IP is becoming the base protocol, most of the telco offers are moving to MPLS. Multi Protocol Layer Switching is a protocol originated by Cisco (the Tag Switching initiative), but now widely adopted.
The chart below briefly summarized the main concepts of MPLS.



In the traditional IP world, every router must route every packet on the network. Routing is rather complex and by the way slow. MPLS introduce (or use) the concepts of tags. Packets are “tagged” at the “entrance” of the WAN. Inside the WAN packets are switched (not routed) based on the tag. Tags are removed at the network exit.

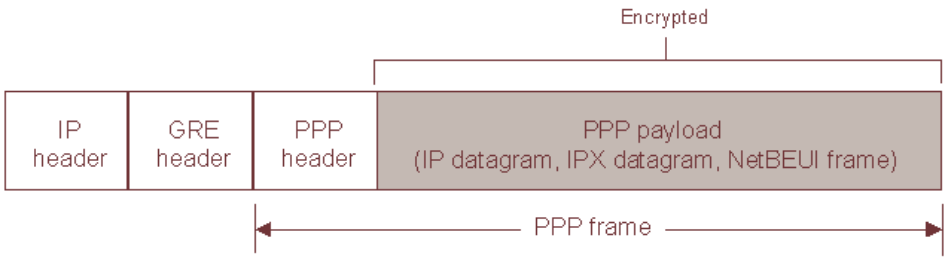
This solution is now widely offered by operators.

The last link layers VPN solution described in this document are L2TP and PPTP. L2TP (Layer 2 Tunnelling Protocol) and PPTP (Point to Point Tunnelling Protocol) are two solutions mainly dedicated to remote access. In the “normal” situation a remote user who wants to connect to the intranet use a PPP connection to a Remote Access Server. In this case, username and password (and also data) are transferred in plain text and therefore might be “sniffed” by potential intruders. L2TP and PPTP permit to encrypt traffic between peers leading to better security

2.2.1.3 PPTP and L2TP

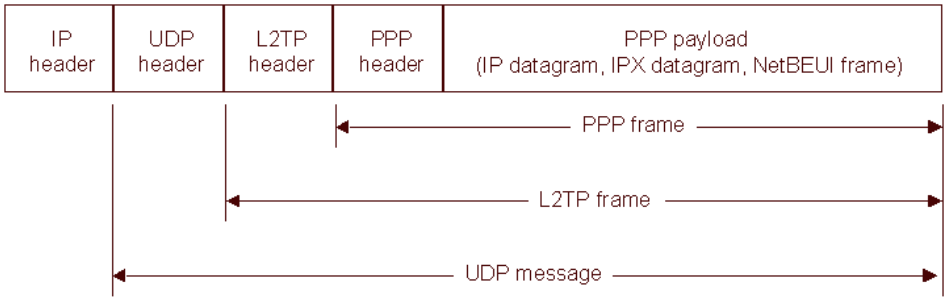
2.2.1.3.1 Point-to-Point Tunneling Protocol (PPTP)

PPTP is a Layer 2 protocol that encapsulates PPP frames in IP datagrams for transmission over an IP internetwork, such as the Internet. PPTP can be used for remote access and router-to-router VPN connections. PPTP is documented in RFC 2637.
The Point-to-Point Tunneling Protocol (PPTP) uses a TCP connection for tunnel maintenance and a modified version of Generic Routing Encapsulation (GRE) to encapsulate PPP frames for tunneled data. The payloads of the encapsulated PPP frames can be encrypted and/or compressed. Figure 6 shows the structure of a PPTP packet containing user data.

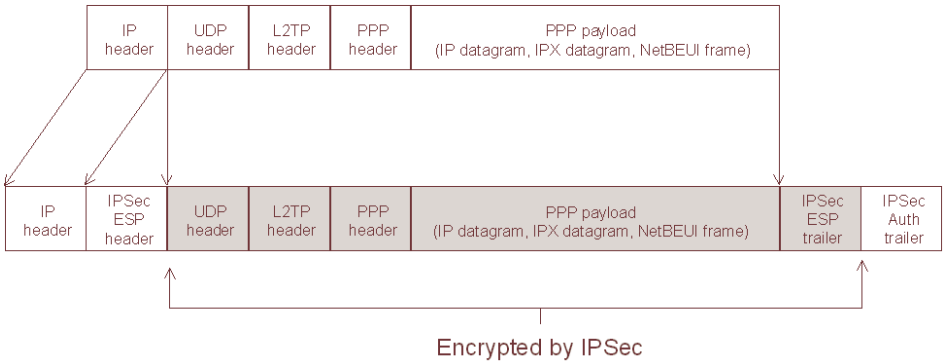


2.2.1.3.2 Layer Two Tunneling Protocol (L2TP)

L2TP is a combination of PPTP and Layer 2 Forwarding (L2F), a technology proposed by Cisco Systems, Inc. L2TP represents the best features of PPTP and L2F. L2TP encapsulates PPP frames to be sent over IP, X.25, Frame Relay, or Asynchronous Transfer Mode (ATM) networks. When configured to use IP as its datagram transport, L2TP can be used as a tunneling protocol over the Internet. L2TP is documented in RFC 2661.
L2TP over IP internetworks uses UDP and a series of L2TP messages for tunnel maintenance. L2TP also uses UDP to send L2TP-encapsulated PPP frames as the tunneled data. The payloads of encapsulated PPP frames can be encrypted and/or compressed.



In Windows 2000, IPSec Encapsulating Security Payload (ESP) is used to encrypt the L2TP packet. This is known as L2TP/IPSec. The result after applying ESP is shown below



2.2.2 Transport and application Layer

These layers covers mainly host based solution.

2.2.2.1 SSL and TSL

Netscape, few years ago, created the protocol SSL (Secure Socket Layer). In the TCP/IP layering model it is on top of the TCP layer.
Therefore, it could be use for adding security (that is strong authentication and encryption) for all TCP-based application (Telnet FTP…).
Some implementations exist for these protocols but the success story of SSL is HTTPS. HTTPS is used in e-commerce application to allow secure information exchanges between client and servers. TSL is the IETF proposed standard equivalent to SSL.

2.2.2.2 SSH

SSH (Secure Shell) is another application layer authentication and encryption protocol. The SSH FAQ (Frequently Asked Question) give the following definition of SSH :

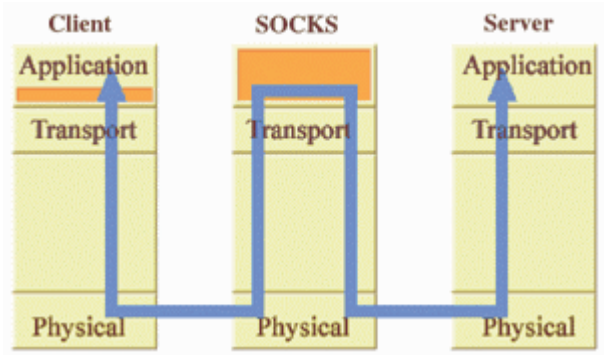
> Secure Shell is a program to log into another computer over a network, to execute commands in a remote machine, and to move files from one machine to another. It provides strong authentication and secure communications over unsecure channels. It is intended as a replacement for telnet, rlogin, rsh, and rcp. For SSH2, there is a replacement for FTP: sftp.

Therefore, the main use of SSH is within organizations. In theory to manage security based devices (firewalls…), or to gain root access on hosts the network/system administrator should avoid to connect remotely using telnet to the box. If telnet is used, it is very easy, with a sniffer, to capture and to analyze the packets to gain administrative access on the firewall/system. With a direct access no clear user/password will be exchange on the LAN. But, network administrators are often lazy… SSH is the answer in this case !
SSH among other things includes an encrypted replacement tool for telnet.

SSH is becoming very popular for secure remote management.

2.2.2.3 SOCKS

SOCKSv5 is an IETF (Internet Engineering Task Force) approved standard (RFC 1928) generic, proxy protocol for TCP/IP-based networking applications. The SOCKS protocol provides a flexible framework for developing secure communications by easily integrating other security technologies.
SOCKS includes two components, the SOCKS server and the SOCKS client. The SOCKS server is implemented at the application layer, while the SOCKS client is implemented between the application and transport layers. The basic purpose of the protocol is to enable hosts on one side of a SOCKS server to gain access to hosts on the other side of a SOCKS Server, without requiring direct IP-reachability.



Socks and the OSI layer model

If SSH is mainly use for secure remote connection, SOCKS is primarily used as a way to provide a secure tunnel between to points and to hide network topology. But, they are both mainly related to client-server exchanges.

2.2.3 So, why IPSEC ?

In the “Guide on the use of TCP/IP on the GTS”, WMO presents two solutions to exchange traffic between MSS using the IP protocol. One is based on FTP and the other on sockets.
This guide does not cover the WAN infrastructure. The current GTS is a mixed of leased lines, peer-to-peer Frame Relay links, global Frame Relay services (like RMDCN in RA VI). For economical reasons, and in regards the overall good quality of service of the Internet, it might be a good opportunity to study the potential use of the Internet to complement the GTS.

However, if reliable (but no real SLA –Service Level Agreement-) the Internet is by nature an insecure network. Various documents within WMO shown how NMCs should connect to the Internet (firewalls…).

In order to allow a smooth introduction of the Internet to complement the GTS the following rules should apply :

- Permit the use of the current protocols (FTP and socket) on the Internet
- Avoid any impact on the MSS
- Guarantee an acceptable level of trust for members

The two first point means that the proposed solution should be transparent to the application and the hosts. Among the protocols describe above, IPSec is the only one completely application independent.

To offer a minimum level of trust, authentication (who wants to talk to me) and encryption (no one except me can understand the data) are both needed. IPSec offers these two services.

3 What is IPSEC ?

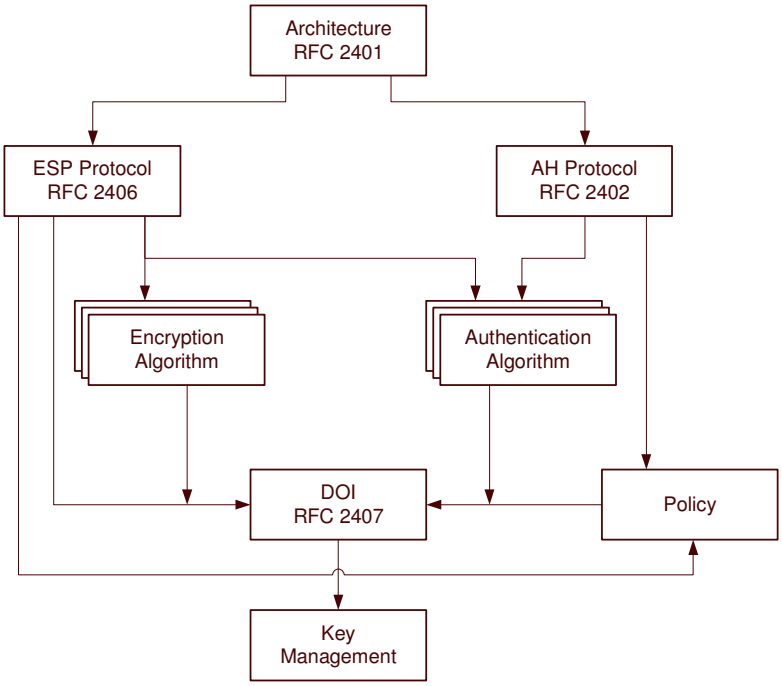
3.1 IPSec architecture

From RFC 2401 :

> **IPSec is designed to provide interoperable high quality, cryptographically-based security for IPv4 and IPv6. The set of security services offered includes access control, connectionless integrity, data origin authentication, protection against replays, confidentiality, and limited traffic flow confidentiality. These services are provided at the IP layer offering protection for the IP and upper layer protocols.**

The IPSec specification is rather complex. The overall architecture of the specification can be seen as a suite of interacting protocols. The RFC2401 gives the organization of the specifications. It can be seen as :

IPSec document overview



• *Architecture* covering the general concepts, security requirements, definitions and mechanisms defining IPSec technology.

- defines the capabilities hosts and routers should provide
- for example, it is required that the hosts provide confidentiality using ESP. However this document does not specify the header format.
- describes the interaction between IPSec and rest of TCP/IP

• *Encapsulation security payload* ESP and *Authentication header* (AH)

- define the protocol, the payload header format and the services they provide.
- define the packet processing rules

- *do not* specify the cryptographic transforms that are used to provide these capabilities. This allows the transforms to be changed if they become cryptographically insecure without any change in the base protocol.

• *Encryption algorithm* and *Authentication algorithm*
- a set of documents that describe how various encryption algorithms are used in ESP or how various authentication algorithms are used in AH and authentication part of ESP.
- defines the algorithm, the key sizes, the derivation of keys, transformation process, any algorithm-specific information.
- the definitions have to be very specific in order to obtain interoperability.

• *Key management* describing the key management schemes.
- keys are generated with Internet Key Exhange (IKE) in IPSec protocols
- The payload format of IKE is very generic. It can be used to negotiate keys in any protocol. IKE is also used for negotiating keys for other protocols outside IPSec.
- The genericity is achieved by separating the parameters IKE negotiates from the protocol itself.

• *Domain of Interpretation* (DOI) contains values needed for the other documents to relate to each other, i.e. identifiers for approved encryption and authentication algorithms, operational parameters like key lifetime.
- the parameters negotiated by IKE are defined in DOI

• *Policy* is an important component
- determines if two entities will be able to communicate with each other, and if so, which transforms to use.
- *Policy representation* deals with definition, storage and retrieval of policy.
- *Policy implementation* addresses the application of policy for actual communication involving e.g. the application of negotiated keys in the communication.

All these documents are RFCs, and as often with RFC, not very readable !!

The following paragraphs introduce IPSec and some key point in it.

3.2 IPSec services and modes

The IPSec framework has been build and defined that way, to guarantee the maximum independence between the different part of the system (encryption algorithm, authentication algorithm… are not linked to ESP and AH protocols for example)
The goal of IPSec is to offer security through encryption and it has been decided to split the solution in several parts. This lead to a very powerful solution, depending on the goal one wants to reach the “good” protocols may be chosen among a large choice. However, it may lead to some incompatibility…
It must also been already noted that in the first design (the first sets of RFCs was published in 1995), the ESP protocol was not usable for authentication. In the second set (published late 1998), the ESP protocol also offers authentication solution.

When two systems want to exchange data using IPSec they must first determine the services they want to use from IPSec. The table below summarize the services offer by ESP and AH.

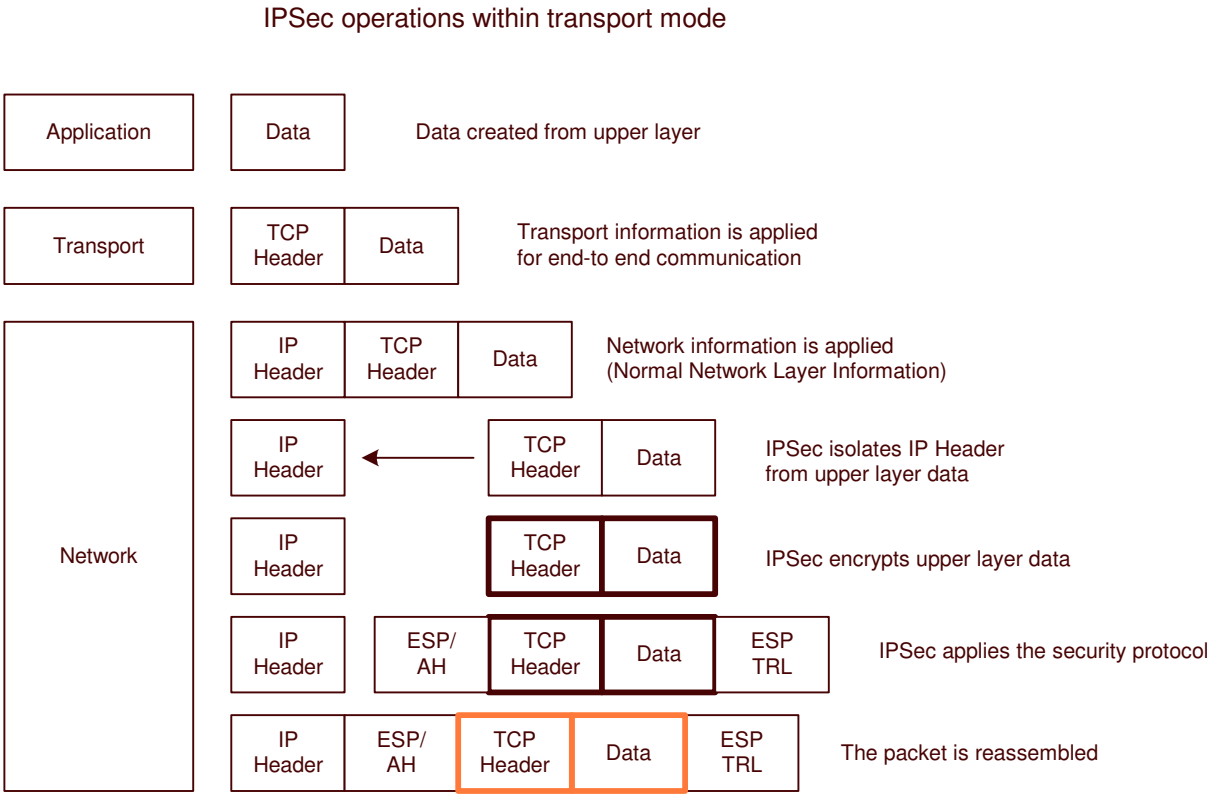
IPSec Services

	AH	ESP (Encryption Only)	ESP (Encryption and authentication)
Access Control	➽	➽	➽
Connectionless Integrity	➽		➽
Data origin authentication	➽		➽

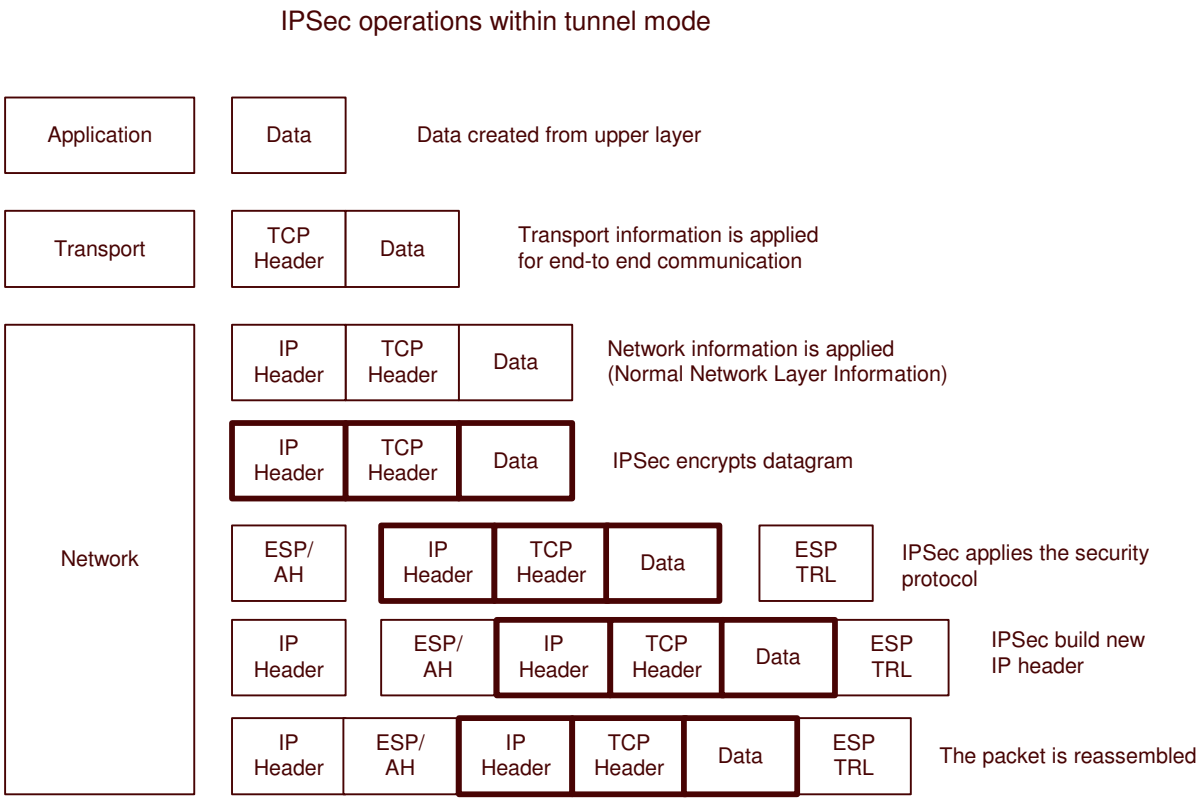
Rejection of replayed packets	➳	➳	➳
Confidentiality		➳	➳
Limited traffic flow confidentiality		➳	➳

This is the first step… but not the last !

Next one, *Tunnel* mode or *Transport* mode. The transport mode is mainly designed for host-to-host communication where IPSec is embedded in the host operating system. In Tunnel mode, the host are not in charge of IPSec, some boxes between the hosts are doing the job.
See below the structure of the packets in the two modes.



In this mode, the real IP header of the packet in used along the way. The IP addresses of the hosts are used to route the packet. It mean that if the packet is going on the Internet, the IP addresses of both hosts must be routable…



The real IP addresses are embedded in the new IPSec packet. If the packet is routed over the Internet, the new IP addresses must be routable.

3.3 Security associations

The security associations or SA in IPSec terminology form the basis for IPSec operations. The SAs are the contracts between two entities determining the IPSec protocols used for securing the packets, the transforms, the keys and their duration plus many other things.
Before two entities are able to exchange packets using IPSec they must first create SAs. SA are always one-way (simplex). So if hosts A and B are communicating with IPSec, each host will have two SA : SA_{in} and SA_{out}. SA_{in} for host A and SA_{out} for host B will share the same cryptographic parameters. Likewise SAs are protocol specific. There is an SA for each protocol : ESP and AH. Each IPSec host therefore has to keep a database (the SADB) to store all SA, the SPI (Security Parameter Index) is a 32-bit element used to identified the SA in the SADB.
SA are managed (created and deleted) either manually or with a protocol, and in this case the protocol used is IKE (Internet Key Exchange).
It is out of the scope of this paper to describe the exact and complete use of SAs but, it must be clear that SAs are the basis of the IPSec framework.

In the framework presented above, SA is linked to “Policy” and “DOI” (Domain Of Interpretation). Security Association is the link between the concepts (IPSec framework) and the reality (how to really use all these things in data communication).

3.4 Authentication Header - AH

AH (Authentication Header) provides data security and authentication of IP packets :

- data integrity ensures that undetected modification to a packet content in transit is not possible
- authentication feature enables end system or network devices to authenticate the user or the application and filter traffic accordingly.

- prevents the address spoofing attacks
- protects against the replay attack

The three first functions are guaranteed by calculation of an authentication hash function. A MAC function (Message Authentication Code) is an authentication process combined with a symmetrical key. To make it short, such function calculates a digest of a message, afterwards the digest is encrypted with a shared secret between the two hosts.

A digest is the result of a fixed length mathematical calculation. It has been proven that is was impossible to recreate the digest if the original information was altered.

Such techniques are used, for example, on public FTP server. When publishing a file on a server, it is useful to also put the digest of the file on the same server. The digest guarantees that the original file has not been modified by anyone.

The most well-known digest calculation method is called MD5.

The required protocols for AH are :
- HMAC-MD5-96
- HMAC-SHA-1-96

The last function in AH (anti-replay attack) is built with a mechanism of sliding window. Each packet receives a sequence number and various techniques guarantee that packet can not be replayed without notice.

3.5 Encapsulating Security Payload - ESP

ESP offers two services :
- encryption : the data is encrypted with a predefined protocol between the two hosts
- authentication : see AH

In the first release of RFC regarding IPSEC, AH was used for authentication and ESP for encryption only. It has been shown by further study, that encryption without authentication was not secure. As, RFCs allow using ESP without AH it was decided to add in the new RFC the capability to authenticate within ESP.

There is now some redundancy ! It is possible to use AH to authenticate, and to use ESP also to authenticate and encrypt. Bruce Shneier, a well-known cryptographic specialist suggest to use ESP for both and to forget about AH…

The authentication algorithm usable in ESP are :
- DES in CBC mode – the only mandatory one
- 3DES
- RC5
- IDEA
- 3 IDEA
- CAST
- Blowfish

DES (Data Encryption Standard) is a rather old protocol developed and promoted by the US government. It has been proven that DES was no more secure. A “brute force” attack could compromise the security of the data encrypted with DES.

NIST (National Institute of Standards and technology) has recently promoted a new protocol AES (Advances Encryption Standard). With the design of IPSec (a collection of separated pieces) AES is going to be rapidly the de-facto standard in IPSec.

3.6 Internet Key Exchange – IKE

In order to talk to each other, peers must use SA. An SA defines the security parameters and authentication keys to use. IKE is the protocol used to create SA.
However, nothing simple in IPSec theory… In fact IKE covers three different protocols :

- ISAKMP – Internet Security Association and Key Management Protocol
- OAKLEY
- SKEME

ISAKMP defines the language for negotiation. It defines the payload format, the mechanics of implementing a key exchange and the negotiation of a security association. ISAKMP does not define the key exchange algorithm but rather the message types in order to exchange keys.
OAKLY and SKEME are two key exchange protocols usable under ISAKMP umbrella in the IKE world.

In fact, ISAKMP, OAKLEY and SKEME were already developed protocol and IKE is a glue between all these.

3.7 Conclusion

In this brief introduction to IPSec, we have seen that :

- Two modes exists : Tunnel and Transport
- Two protocols partially redundant are defined : ESP and AH
- Security Association are created and maintained by three different protocols
- Authentication can be achieve through two possible algorithms
- Encryption rely on DES (which is insecure) and 6 others protocols. A new one AES will probable overcome all others

We have neither covered nor introduced other aspects which may also be relevant in IPSec :

- Diffie-Helmann protocol to create keys
- Certificates
- PKI –Public Key Infrastructure
- …

VPN, in some aspect, is quite a vague concept, IPSec, one of the VPN solution is not much clear !

So, despite the rather ugly face of the protocol, the various options, the risk of incompatibility, IPSec is now widely implemented and available on a lot of platform, including, routers, dedicated boxes, firewalls, hosts…

In fact, in most cases, the solutions implemented only cover a part of the possible options. It is therefore, very important to guarantee interoperability to share the same subset among the peers.

In the following part, we suggest a possible scenario taking into account the need of security, some legal aspects and interoperability issues.

4 IPSEC and the GTS

4.1 Cryptography and the law

In VPNs and also in IPSec, cryptography is one of the key point to ensure privacy of the communication. The government in all the countries have and still do consider cryptography as some sort of weapon.
It has often be explained by different government in the world, that lawful activities perhaps needs privacy but, the main use of crypto tools was for unlawful activities. Therefore, every country has defined rules about the use of cryptography within the country.
The web site http://rechten.kub.nl/koops/cryptolaw/ presents the situation regarding cryptography in a lot of countries (from the web site) :

> In the last years a group of countries worked on the Wassenaar Arrangement. It controls the export of weapons and of dual-use goods, that is, goods that can be used both for a military and for a civil purpose; cryptography is such a dual-use good.
> In 1995, 28 countries decided to establish a follow-up to COCOM, the *Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies*. The negotiations on the Arrangement were finished in July 1996, and the agreement was signed by 31 countries (Argentina, Australia, Austria, Belgium, Canada, the Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Japan, Luxembourg, the Netherlands, New Zealand, Norway, Poland, Portugal, the Republic of Korea, Romania, the Russian Federation, the Slovak Republic, Spain, Sweden, Switzerland, Turkey, the United Kingdom and the United States). Later, Bulgaria and Ukraine also became a participating state to the Arrangement.
> The initial provisions were largely the same as old COCOM regulations. The General Software Note (applicable until the December 1998 revision) excepted mass-market and public-domain crypto software from the controls. Australia, France, New Zealand, Russia, and the US deviated from the GSN and controlled the export of mass-market and public-domain crypto software. Export via the Internet did not seem to be covered by the regulations.
> There is a personal-use exemption, allowing export of products "accompanying their user for the user's personal use" (e.g., on a laptop).
> The Wassenaar Arrangement was revised in December 1998. Negotiations were held on 2 and 3 December 1998 in Vienna, which resulted in restrictions on the General Software Note and in some relexations:
> - free for export are: all symmetric crypto products of up to 56 bits, all asymmetric crypto products of up to 512 bits, and all subgroup-based crypto products (including elliptic curve) of up to 112 bits;
> - mass-market symmetric crypto software and hardware of up to 64 bits are free for export (the 64-bit limit was deleted on 1 December 2000, see below);
> - the export of products that use encryption to protect intellectual property (such as DVDs) is relaxed;
> - export of all other crypto still requires a license

DES protocol uses a 56 bits key. It is therefore legal in most countries. But 3DES, which is equivalent to a 168-bit key, is often out-of-law.

.

Before any use of cryptographic solution, everyone and especially government agencies such as National Meteorological Centres MUST verify if the solution they want to use are legal in their country

4.2 A quick view on the GTS

4.2.1 Physical layer

The current GTS is a mixed of various technical solutions :

- leased line, the most common but for sure not the less expensive solution in case of international circuits
- Frame-Relay lines. The leased line is replaced by a connection to a Frame Relay network but only two peers share the same Frame Relay network.
- Frame Relay network. A group of countries share the same operated network and agreed on a technical and commercial global solution. The RMDCN in region VI is such a network

The reproaches for the three solutions are quite the same :

- costs : for (relatively) slow speed lines the price are high
- either the leased line or the PVCs in Frame Relay are one-to-one link and therefore works well for one-to-one communication, but neither for many-to-many nor any-to-any dialog are convenient.

But, the current needs on telecommunication become higher and higher in terms of :

- traffic
- global exchange

With the growth of products and datas, NMCs want to exchange much more information. The current architecture based on concentration through RTHs and costly slow speed line is not enough opened to allow such an evolution.

4.2.2 Upper layers

The “Guide on the use of TCP/IP on the GTS” describes how to use IP as a replacement of the legacy X25 protocol. The future of the GTS is IP and technical evolution on the network should be searched in the IP direction.

At the application layer, two protocols are usable above the IP layer : FTP and sockets. Every new solution must conform to these standards.

4.3 The Internet

Most NMCs are now connected to the Internet. The Internet connection is in most cases :

- reliable. The ISP (Internet Service Providers) propose connection to the Internet. They are operated just like others leased lines and are therefore as reliable as the lines. However it must be noted that no end-to-end SLA (Service Level Agreement) could be defined on the Internet.
- powerful. The Internet connection is often a high speed connection.
- secured. The NMCs should (and even must) be protected by firewalls.

Therefore, the Internet is becoming a possible media to complement the current GTS private infrastructure.

4.4 The suggested approach

As seen before, the only real application and host independent VPN solution is IPSec.

Therefore, for WMO use we recommend IPSec as the VPN solution.

But in order to guarantee interoperability between NMCs without redefining each time the protocols to use we suggest the following implementation solution :

- Tunnel mode : as IPSec will be the most probably configured on routers, firewall or dedicated boxes, and taking into account that neither encryption nor authentication are mandatory on LAN, Tunnel mode is the most appropriate solution
- AH (Authentication Header) should not be used

- ESP (Encapsulting Security Paylod) is used for both authentication and encryption
    - Authentication should be done with HMAC-MD5-96
    - Encryption should be done with DES
- Pre-Shared secrets : Certificated is probably a more elegant solution, but, in practical, more difficult to implement in WMO situation.

These recommendations mostly come from “A cryptographic evaluation of IPSec” form Couterpane (http://www.counterpane.com/ipsec.html).

The main difference is the choice of DES. In the RFCs DES is the only mandatory protocol for encryption. Others are optional.

Specialists in cryptography recommend forgetting DES, because it is insecure.

4.4.1 Why DES must not be chosen !

The following come from FreeSwan (http://ww.freeswan.org) web site, a free implementation of IPSec.

> **DES is Not Secure**
>
> DES, the Data Encryption Standard, can no longer be considered secure. While no major flaws in its innards are known, it is fundamentally inadequate because its 56-bit key is too short. It is vulnerable to brute-force search of the whole key space, either by large collections of general-purpose machines or even more quickly by specialized hardware. Of course this also applies to any other cipher with only a 56-bit key. The only reason anyone could have for using a 56 or 64-bit key is to comply with various export laws intended to ensure the use of breakable ciphers.
>
> Non-government cryptologists have been saying DES's 56-bit key was too short for some time -- some of them were saying it in the 70's when DES became a standard -- but the US government has consistently ridiculed such suggestions.
>
> A group of well-known cryptographers looked at key lengths in a 1996 paper. They suggested a minimum of 75 bits to consider an existing cipher secure and a minimum of 90 bits for new ciphers. More recent papers, covering both symmetric and public key systems are at cryptosavvy.com and rsa.com. For all algorithms, the minimum keylengths recommended in such papers are significantly longer than the maximums allowed by various export laws.
>
> In a 1998 ruling, a German court described DES as "out-of-date and not safe enough" and held a bank liable for using it.
> Dedicated hardware breaks DES in a few days
>
> The question of DES security has now been settled once and for all. In early 1998, the Electronic Frontier Foundation built a DES-cracking machine. It can find a DES key in an average of a few days' search. The details of all this, including complete code listings and complete plans for the machine, have been published in Cracking DES, by the Electronic Frontier Foundation.
>
> That machine cost just over $200,000 to design and build. "Moore's Law" is that machines get faster (or cheaper, for the same speed) by roughly a factor of two every 18 months. At that rate, their $200,000 in 1998 becomes $50,000 in 2001.
>
> However, Moore's Law is not exact and the $50,000 estimate does not allow for the fact that a copy based on the published EFF design would of course cost far less than the original. We cannot say exactly what such a cracker would cost today, but it would likely be somewhere between $10,000 and $100,000.

4.4.2 However DES !

The above analysis is true. DES is breakable. But, we think that for WMO community DES is enough. Enough for at least two reasons :

- the encryption algorithm must be lawful in most countries. To make it simple, it means that the encryption keys must be short.
- the data to be protected even valuable for NMCs, are probably not the one a cracker would try to break.

4.5 Solution suppliers

With the subset of protocols defined above, each NMCs can choose any supplier for VPNs equipment.

Of course, Cisco is a solution.
Cisco offers on VPN is very widespread :

- router with software encryption
- router with hardware incryption
- firewalls
- dedicated boxes

But others, like Nortel, CheckPoint… have also technical solution.

All IPSec implementation should be compatible. But, as seen above, IPSec offers a large choice. The solution proposed in 4.4 is included in the mandatory subset of protocols described in the RFCs. So any RFC compliant solution should interoperate with others. In very infrequent cases it might not be true. So before choosing a VPN box, NMCs should check with potential VPN neighbor if their respective solutions are compatible. This information can be found on the web.

4.6 Implementation scenario

In order for two NMCs to establish a VPN link they must :

- confirm the protocols to be used (confirm use of tunnel mode, DES, MD5, pre-shared secrets)
- define the pres-shared secret. This "password" must be define and be the same on both sides
- confirm the VPN platform to be used
- agree on IP addresses to exchange on the link
- modify filter rules on the firewall. The following rules
    - UDP port 500 is used for ISAKMP
    - IP protocol number 50 (ESP protocol)
- implement the define configuration
- test

Once everything running, the main risk is the potential failure of the virtual link created.

5 Operators solutions

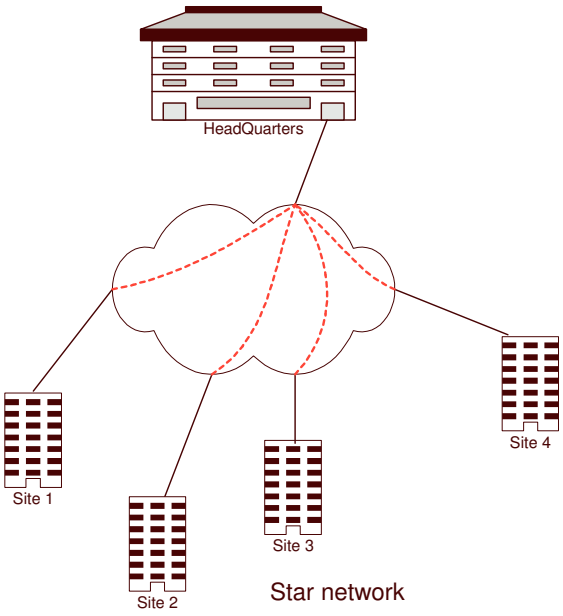
In the recent past years operator market for shared networks consist mainly in :

- Frame Relay for “slow” lines (up to few mb/s)
- ATM for higher speed communication.

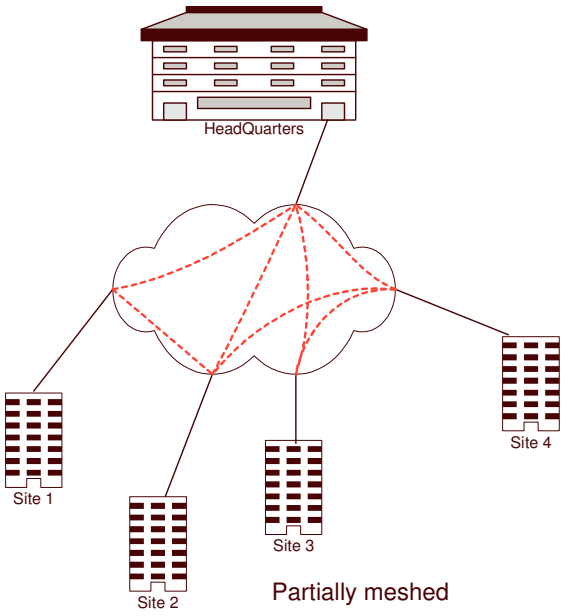
These two solutions are layer 2 based, and therefore are completely independent of level 3 protocols. However, as IP is the universal layer 3 protocol, technical alternatives solutions are offered.

The main disadvantage of Frame Relay and ATM are their static nature. The client must define exactly what peers are allowed to exchange traffic and the throughput they want. These solutions are not flexible. It is costly and often create administrative complexity o change the parameters and to allow a more dynamic approach.

5.1 Star, partially meshed, fully meshed networks



Star network

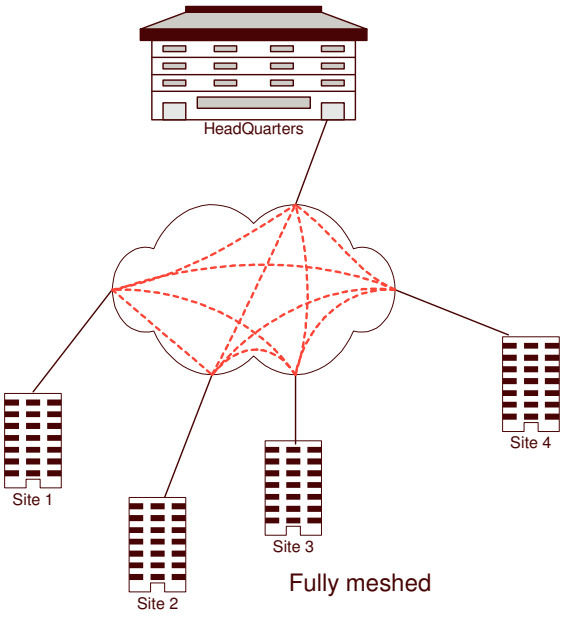


Partially meshed

Either in Frame Relay or in ATM, the client must choose between :

- star network
- partially meshed
- fully meshed

The choice is based on cost considerations (the price of these network is often linked to numbers of PVCs and their speed) and traffic analysis.
It is often desirable to have more PVCs but thus increasing the cost of the total network.
In the case of RMDCN for example it was decided to minimize the number of PVCs but, for less often communications, ECMWF offers Electronic Traffic Routing. Therefore, the total solution is a mixed between operator service and self operated service.



Fully meshed

5.2 Technical solutions

Based on current infrastructure, Frame Relay and ATM, operators have new IP based services :

- MPLS VPN
- IPSec VPN

Of course, in both cases, just like with Frame Relay or ATM, the traffic from one client is isolated from the others. Therefore, the client has a Virtual Private Network.

5.2.1 MPLS

MPLS is seen by the operators as a way to propose to their clients high speed communication in a more manageable way compare to traditional solution. Based on their current Frame Relay or ATM network, MPLS is an easier way to propose a partially meshed or a fully meshed network, and therefore, the network should be cheaper.

First experiences in Europe, however, show that the cost in not so different than with previous solutions !!

Some others services, like priorities might be proposed on MPLS networks.

5.2.2 IPSec VPN

The Internet is a collection of interconnected IPSs networks. Each ISP owns its infrastructure and interconnects with others to provide Internet access to its clients.
Within its network, an ISP can guarantee a level of service and therefore, with add-on can propose to build a VPN based on IPSec. In this case, VPN is a value added service on top of Internet connection.

But, as seen above in IPSec section, every connection must be manually created.

5.3 Conclusion

For the MTN or regional network, operators solutions offer guarantee of service, guaranteed bandwidth. But whatever the technology the problems stay the same :

- the cost : an MPLS network is more expensive than a star Frame Relay solution (but probably cheaper than fully meshed)
- the same operator must be available on every site.
- the problem of administrative cost sharing remain the same

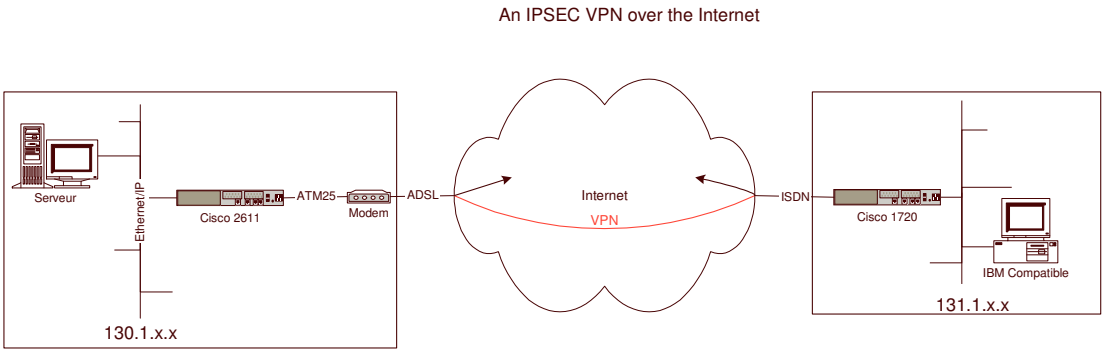
The underlying technology for operators services is important but, this is not the first issue to consider.

6 Appendices

6.1 A Cisco based configuration

6.1.1 The test platform

This test platform aims to demonstrate the connection of two Cisco routers using IPSEC over the Internet.



Both sites are connected to the Internet. The left one (see above) is connected through a permanent ADSL connection. The right one connects through ISDN.
Both site musts keep normal Internet access. Internet accesses are not dedicated to IPSEC connection, and depending on destination the connection must be direct or use the ad-hoc VPN.
ADSL site must have a permanent IP address on the ADSL side of the router. ISDN site receive a dynamic IP address for every new connection. NAT (Network Address Translation) is used to masquerade internal IP addresses.

6.1.2 ADSL connection with NAT

In order to understand the step-by-step connection mecanism we first indicate the ADSL connexion including NAT. In this case, there is no IPSEC.

```
!
version 12.1
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname ADSL
!
enable secret 5 $1$zuPR$fsH7hiZKiW3ePfCXlBAAg.
enable password PWD
!
username UserNetissimo password 0 PwdNetissimo
!
memory-size iomem 15
ip subnet-zero
no ip finger
!
!
interface Ethernet0/0
 ip address 130.1.8.1 255.255.0.0
 ip nat inside
!
interface Ethernet0/1
 no ip address
 shutdown
!
interface ATM1/0
 no ip address
 atm vc-per-vp 4096
```

```
 no atm ilmi-keepalive
 pvc 2/32
  encapsulation aal5mux ppp Virtual-Template1
 !
interface Virtual-Template1
 ip address negotiated
 no ip redirects
 no ip proxy-arp
 ip nat outside
 pulse-time 0
 ppp chap hostname UserNetissimo
 ppp chap password 7 00574404035D1207
 no ppp chap wait
 ppp pap sent-username UserNetissimo password 7 04085C040827554F
!
ip nat pool NET 193.253.191.14 193.253.191.14 netmask 255.255.255.0
ip nat inside source list 1 pool NET overload
ip classless
ip route 0.0.0.0 0.0.0.0 193.253.191.1
ip http server
!
access-list 1 permit any
!
line con 0
 transport input none
line aux 0
line vty 0 4
 password PWD
 login
!
no scheduler allocate
end
```

6.1.3 VPN between the routers

ADSL Router :

```
!
version 12.1
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname ADSL
!
enable secret 5 $1$zuPR$fsH7hiZKiW3ePfCXlBAAg.
enable password PWD
!
username UserNetissimo password 0 PwdNetissimo
!
memory-size iomem 15
ip subnet-zero
no ip finger
!
crypto isakmp policy 1
 hash md5
 authentication pre-share
crypto isakmp key IPSECKEY address 0.0.0.0
!
crypto ipsec transform-set CMT esp-des esp-md5-hmac
!
crypto dynamic-map MYMAP 10
 set security-association lifetime seconds 600
 set transform-set CMT
 match address 100
!
crypto map CMMYMAP 30 ipsec-isakmp dynamic MYMAP discover
!
interface Ethernet0/0
 ip address 130.1.8.1 255.255.0.0
!
interface Ethernet0/1
 no ip address
 shutdown
!
interface ATM1/0
 no ip address
 atm vc-per-vp 4096
 no atm ilmi-keepalive
 pvc 2/32
```

```
  encapsulation aal5mux ppp Virtual-Template1
!
interface Virtual-Template1
 ip address negotiated
 no ip redirects
 no ip proxy-arp
 pulse-time 0
 ppp chap hostname UserNetissimo
 ppp chap password 7 00574404035D1207
 no ppp chap wait
 ppp pap sent-username UserNetissimo password 7 04085C040827554F
 crypto map CMMYMAP
!
ip classless
ip route 0.0.0.0 0.0.0.0 193.253.191.1
ip http server
!
access-list 1 permit any
access-list 100 permit ip 130.1.0.0 0.0.255.255 131.1.0.0 0.0.255.255
!
line con 0
 transport input none
line aux 0
line vty 0 4
 password PWD
 login
!
end
```

ISDN Router :

```
version 12.1
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname ISDN
!
enable secret 5 $1$n6eZ$UXI24gGl7lZu/wB3OZVnC1
enable password PWD
!
memory-size iomem 25
ip subnet-zero
no ip finger
no ip domain-lookup
!
isdn switch-type vn3
!
crypto isakmp policy 1
 hash md5
 authentication pre-share
crypto isakmp key IPSECKEY address 193.253.191.14
!
crypto ipsec transform-set CMT esp-des esp-md5-hmac
!
crypto map CMYMAP 1 ipsec-isakmp
 set peer 193.253.191.14
 set security-association lifetime seconds 600
 set transform-set CMT
 match address 100
!
cns event-service server
!
interface BRI0
 no ip address
 encapsulation ppp
 no ip mroute-cache
 dialer pool-member 1
 isdn switch-type vn3
 isdn send-alerting
 no cdp enable
 crypto map CMYMAP
!
interface FastEthernet0
 ip address 131.1.8.1 255.255.0.0
 no ip mroute-cache
 speed auto
 full-duplex
!
interface Dialer0
 ip address negotiated
```

```
 encapsulation ppp
 dialer remote-name LibertySurf
 dialer pool 1
 dialer string 0860155555
 dialer-group 1
 pulse-time 0
 no cdp enable
 ppp authentication chap pap callin
 ppp chap hostname bane0000@lsurf.fr
 ppp chap password 7 1307160B04020A2F
 ppp pap sent-username bane0000@lsurf.fr password 7 14151312030A242E
 crypto map CMYMAP
!
ip classless
ip route 0.0.0.0 0.0.0.0 Dialer0
no ip http server
!
access-list 1 permit any
access-list 100 permit ip 131.1.0.0 0.0.255.255 130.1.0.0 0.0.255.255
dialer-list 1 protocol ip permit
!
line con 0
 transport input none
line aux 0
line vty 0 4
 password PWD
 login
!
no scheduler allocate
end
```

In the two configuration the red and underlines lines show the IPSEC set-up. Let's focuses on this part of the configuration.

ADSL	ISDN
crypto isakmp policy 1 hash md5 authentication pre-share crypto isakmp key IPSECKEY address 0.0.0.0 ! crypto ipsec transform-set CMT esp-des esp-md5-hmac ! crypto dynamic-map MYMAP 10 set security-association lifetime seconds 600 set transform-set CMT match address 100 ! crypto map CMMYMAP 30 ipsec-isakmp dynamic MYMAP discover ! access-list 100 permit ip 130.1.0.0 0.0.255.255 131.1.0.0 0.0.255.255 ! interface ATM1/0 crypto map CMMYMAP !	crypto isakmp policy 1 hash md5 authentication pre-share crypto isakmp key IPSECKEY address 193.253.191.14 ! crypto ipsec transform-set CMT esp-des esp-md5-hmac ! crypto map CMYMAP 1 ipsec-isakmp set peer 193.253.191.14 set security-association lifetime seconds 600 set transform-set CMT match address 100 ! access-list 100 permit ip 131.1.0.0 0.0.255.255 130.1.0.0 0.0.255.255 ! interface Dialer0 crypto map CMYMAP

6.1.3.1 IKE

In the configuration, this is related to the lines :

```
crypto isakmp policy 1
 hash md5
 authentication pre-share
crypto isakmp key IPSECKEY address 0.0.0.0
```

The protocol used for IKA is isakmp and it has been established a pre-shared secret. This secret will be used by both router to exchanges real encryption key.
IPSECKEY is the secret shared between the two routers.
On ADSL side, the originate IP address of the ISDN router is not known (in dialup connection like ISDN this address will change for every new connection) therefore at this stage the 0.0.0.0 mean accept this IPSECKEY for every address. This may lead to potential security risk. We will see below how Cisco permit to minimize it.

6.1.3.2 AH et ESP

The Authentication header protocol and the encapsulation security payload is then selected. Depending on the hashing protocol available, the encryption solution, the choice to rely on ESP for both authentication and encryption or to AH, the line :

```
crypto ipsec transform-set CMT esp-des esp-md5-hmac
```

describes which protocols are to be used for this particular IPSEC VPN. In our case, ESP is the preferred method for both authentication and encryption.
ESP-DES means use DES for ESP (this is encryption). ESP-MD5-HMAC means use MD5-HMAC for authentication with ESP. Of course the choice must be the same for both sides of the tunnel.

6.1.3.3 Security Association

The first two parts show the protocol part, let's now work on Security Association. The ADSL must accept incoming IPSEC connection from unknown peer :

```
crypto dynamic-map MYMAP 10
 set security-association lifetime seconds 600
 set transform-set CMT
 match address 100
!
crypto map CMMYMAP 30 ipsec-isakmp dynamic MYMAP discover
!
access-list 100 permit ip 130.1.0.0 0.0.255.255 131.1.0.0 0.0.255.255
```

Therefore, Cisco offer the "dynamic-map" solution. In this case, the ADSL router will accept every new connection using the right protocols (esp-des and esp-md5-hmac) from any IP address using the right password IPSECKEY. In order to restrict the use of this IPSEC tunnel Cisco use the mecanism of access-list. The access-list 100 must be the same on both side of the tunnel in order to allow the IPSEC connection. This is a Cisco dependant feature.

6.1.4 Final configuration

A mixed of above configuration NAT and IPSEC are gathered in one configuration.

ADSL Router :

```
!
version 12.1
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname ADSL
!
enable secret 5 $1$zuPR$fsH7hiZKiW3ePfCXlBAAg.
enable password PWD
!
username UserNetissimo password 0 PwdNetissimo
!
memory-size iomem 15
ip subnet-zero
no ip finger
!
crypto isakmp policy 1
 hash md5
 authentication pre-share
crypto isakmp key IPSECKEY address 0.0.0.0
!
crypto ipsec transform-set CMT esp-des esp-md5-hmac
!
crypto dynamic-map MYMAP 10
 set security-association lifetime seconds 600
 set transform-set CMT
 match address 100
!
crypto map CMMYMAP 30 ipsec-isakmp dynamic MYMAP discover
!
interface Ethernet0/0
 ip address 130.1.8.1 255.255.0.0
 ip nat inside
!
interface Ethernet0/1
 no ip address
```

```
 shutdown
!
interface ATM1/0
 no ip address
 atm vc-per-vp 4096
 no atm ilmi-keepalive
 pvc 2/32
  encapsulation aal5mux ppp Virtual-Template1
!
interface Virtual-Template1
 ip address negotiated
 no ip redirects
 no ip proxy-arp
 ip nat outside
 pulse-time 0
 ppp chap hostname UserNetissimo
 ppp chap password 7 00574404035D1207
 no ppp chap wait
 ppp pap sent-username UserNetissimo password 7 04085C040827554F
 crypto map CMMYMAP
!
ip nat pool NET 193.253.191.14 193.253.191.14 netmask 255.255.255.0
ip nat inside source list 101 pool NET overload
ip classless
ip route 0.0.0.0 0.0.0.0 193.253.191.1
ip http server
!
access-list 1 permit any
access-list 100 permit ip 130.1.0.0 0.0.255.255 131.1.0.0 0.0.255.255
access-list 101 deny   ip 130.1.0.0 0.0.255.255 131.1.0.0 0.0.255.255
access-list 101 permit ip any any
!
line con 0
 transport input none
line aux 0
line vty 0 4
 password PWD
 login
!
end
```

ISDN Router :

```
!
version 12.1
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname ISDN
!
enable secret 5 $1$n6eZ$UXI24gGl7lZu/wB3OZVnC1
enable password PWD
!
memory-size iomem 25
ip subnet-zero
no ip finger
no ip domain-lookup
!
isdn switch-type vn3
!
crypto isakmp policy 1
 hash md5
 authentication pre-share
crypto isakmp key CléIPSEC address 193.253.191.14
!
crypto ipsec transform-set CMT esp-des esp-md5-hmac
!
crypto map CMYMAP 1 ipsec-isakmp
 set peer 193.253.191.14
 set security-association lifetime seconds 600
 set transform-set CMT
 match address 100
!
cns event-service server
!
interface BRI0
 no ip address
 ip nat outside
 encapsulation ppp
 no ip mroute-cache
```

```
 dialer pool-member 1
 isdn switch-type vn3
 isdn send-alerting
 no cdp enable
 crypto map CMYMAP
!
interface FastEthernet0
 ip address 131.1.8.1 255.255.0.0
 ip nat inside
 no ip mroute-cache
 speed auto
 full-duplex
!
interface Dialer0
 ip address negotiated
 encapsulation ppp
 dialer remote-name LibertySurf
 dialer pool 1
 dialer string 0860155555
 dialer-group 1
 pulse-time 0
 no cdp enable
 ppp authentication chap pap callin
 ppp chap hostname bane0000@lsurf.fr
 ppp chap password 7 1307160B04020A2F
 ppp pap sent-username bane0000@lsurf.fr password 7 14151312030A242E
 crypto map CMYMAP
!
interface Dialer1
 ip address negotiated
 ip nat outside
 encapsulation ppp
 dialer pool 1
 dialer string 0860155555
 dialer-group 1
 pulse-time 0
 no cdp enable
 ppp authentication chap pap callin
 ppp chap hostname bane0000@lsurf.fr
 ppp chap password 7 1307160B04020A2F
 ppp pap sent-username bane0000@lsurf.fr password 7 14151312030A242E
!
ip nat inside source list 101 interface Dialer1 overload
ip classless
ip route 0.0.0.0 0.0.0.0 Dialer1
ip route  130.1.0.0 255.255.0.0 Dialer0
ip route 193.253.191.14 255.255.255.255 Dialer0
no ip http server
!
access-list 1 permit any
access-list 100 permit ip 131.1.0.0 0.0.255.255 130.1.0.0 0.0.255.255
access-list 101 deny   ip 131.1.0.0 0.0.255.255 130.1.0.0 0.0.255.255
access-list 101 permit ip any any
dialer-list 1 protocol ip permit
!
line con 0
 transport input none
line aux 0
line vty 0 4
 password PWD
 login
!
end
```

6.2 Glossary

The following glossary is based on http://www.freeswan.org/freeswan_trees/freeswan-1.95/doc/glossary.html

3DES (Triple DES)
: Using three DES encryptions on a single data block, with at least two different keys, to get higher security than is available from a single DES pass.
IPsec always does 3DES with three different keys, as required by RFC 2451. For an explanation of the two-key variant, see two key triple DES. Both use an EDE encrypt-decrypt-encrpyt sequence of operations.
Single DES is insecure.

Double DES is ineffective. Using two 56-bit keys, one might expect an attacker to have to do 2112 work to break it. In fact, only 257 work is required with a meet-in-the-middle attack, though a large amount of memory is also required. Triple DES is vulnerable to a similar attack, but that just reduces the work factor from the 2168 one might expect to 2 112. That provides adequate protection against brute force attacks, and no better attack is known.

3DES can be somewhat slow compared to other ciphers. It requires three DES encryptions per block. DES was designed for hardware implementation and includes some operations which are difficult in software. However, the speed we get is quite acceptable for many uses. See our performance document for details.

AES

The Advanced Encryption Standard, a new block cipher standard to replace DES being developed by NIST, the US National Institute of Standards and Technology. DES used 64-bit blocks and a 56-bit key. AES ciphers use a 128-bit block and are required to support 128, 192 and 256-bit keys. Some of them support other sizes as well. The larger block size helps resist birthday attacks while the large key size prevents brute force attacks.

Fifteen proposals meeting NIST's basic criteria were submitted in 1998 and subjected to intense discussion and analysis, "round one" evaluation. In August 1999, NIST narrowed the field to five "round two" candidates:

· Mars from IBM
· RC6 from RSA
· Rijndael from two Belgian researchers
· Serpent, a British-Norwegian-Israeli research collaboration
· Twofish from the consulting firm Counterpane

Three of the five finalists -- Rijndael, Serpent and Twofish -- have completely open licenses.

In October 2000, NIST announced the winner -- Rijndael.

For more information, see:

· NIST's AES home page
· the Block Cipher Lounge AES page
· Brian Gladman's code and benchmarks
· Helger Lipmaa's survey of implementations

Adding one or more AES ciphers to Linux FreeS/WAN would be a useful undertaking. Likely one would add all three of the Round Two candidates with good licenses. A complication is that our code is built for a 64-bit block cipher and AES uses a 128-bit block. Volunteers via the mailing lists would be welcome.

AH

The IPsec Authentication Header, added after the IP header. For details, see IPsec document and/or RFC 2402.

Asymmetric cryptography

See public key cryptography.

Authentication

Ensuring that a message originated from the expected sender and has not been altered on route. IPsec uses authentication in two places:

· peer authentication, authenticating the players in IKE's Diffie-Hellman key exchanges to prevent man-in-the-middle attacks. This can be done in a number of ways. The methods supported by FreeS/WAN are discussed in our configuration document.

· packet authentication, authenticating packets on an established SA, either with a separate authentication header or with the optional authentication in the ESP protocol. In either case, packet authentication uses a hashed message athentication code technique.

Outside IPsec, passwords are perhaps the most common authentication mechanism. Their function is essentially to authenticate the person's identity to the system. Passwords are generally only as secure as the network they travel over. If you send a cleartext password over a tapped phone line or over a network with a packet sniffer on it, the security provided by that password becomes zero. Sending an encrypted password is no better; the attacker merely records it and reuses it at his convenience. This is called a replay attack.

A common solution to this problem is a challenge-response system. This defeats simple eavesdropping and replay attacks. Of course an attacker might still try to break the cryptographic algorithm used, or the random number generator.

Birthday attack

A cryptographic attack based on the mathematics exemplified by the birthday paradox. This math turns up whenever the question of two cryptographic operations producing the same result becomes an issue:

· collisions in message digest functions.

· identical output blocks from a block cipher
· repetition of a challenge in a challenge-response system

Resisting such attacks is part of the motivation for:

· hash algorithms such as SHA and RIPEMD-160 giving a 160-bit result rather than the 128 bits of MD4, MD5 and RIPEMD-128.
· AES block ciphers using a 128-bit block instead of the 64-bit block of most current ciphers
· IPsec using a 32-bit counter for packets sent on an automatically keyed SA and requiring that the connection always be rekeyed before the counter overflows.

Birthday paradox

Not really a paradox, just a rather counter-intuitive mathematical fact. In a group of 23 people, the chance of a least one pair having the same birthday is over 50%.

The second person has 1 chance in 365 (ignoring leap years) of matching the first. If they don't match, the third person's chances of matching one of them are 2/365. The 4th, 3/365, and so on. The total of these chances grows more quickly than one might guess.

Block cipher

A symmetric cipher which operates on fixed-size blocks of plaintext, giving a block of ciphertext for each. Contrast with stream cipher. Block ciphers can be used in various modes when multiple block are to be encrypted.

DES is among the the best known and widely used block ciphers, but is now obsolete. Its 56-bit key size makes it highly insecure today.

The current generation of block ciphers -- such as Blowfish, CAST-128 and IDEA -- all use 64-bit blocks and 128-bit keys. The next generation, AES, uses 128-bit blocks and supports key sizes up to 256 bits.

The Block Cipher Lounge web site has more information.

Blowfish

A block cipher using 64-bit blocks and keys of up to 448 bits, designed by Bruce Schneier and used in several products.

This is not required by the IPsec RFCs

Brute force attack (exhaustive search)

Breaking a cipher by trying all possible keys. This is always possible in theory (except against a one-time pad), but it becomes practical only if the key size is inadequate. For an important example, see our document on the insecurity of DES with its 56-bit key. For an analysis of key sizes required to resist plausible brute force attacks, see this paper.

Longer keys protect against brute force attacks. Each extra bit in the key doubles the number of possible keys and therefore doubles the work a brute force attack must do. A large enough key defeats any brute force attack.

For example, the EFF's DES Cracker searches a 56-bit key space in an average of a few days. Let us assume an attacker that can find a 64-bit key (256 times harder) by brute force search in a second (a few hundred thousand times faster). For a 96-bit key, that attacker needs 232 seconds, about 135 years. Against a 128-bit key, he needs 232 times that, over 500,000,000,000 years. Your data is then obviously secure against brute force attacks. Even if our estimate of the attacker's speed is off by a factor of a million, it still takes him over 500,000 years to crack a message.

This is why

· single DES is now considered dangerously insecure
· all of the current generation of block ciphers use a 128-bit or longer key
· AES ciphers support keysizes 128, 192 and 256 bits
· any cipher we add to Linux FreeS/WAN will have at least a 128-bit key

Cautions:

Inadequate keylength always indicates a weak cipher but it is important to note that adequate keylength does not necessarily indicate a strong cipher. There are many attacks other than brute force, and adequate keylength only guarantees resistance to brute force. Any cipher, whatever its key size, will be weak if design or implementation flaws allow other attacks.

Also, once you have adequate keylength (somewhere around 90 or 100 bits), adding more key bits make no practical difference , even against brute force. Consider our 128-bit example above that takes 500,000,000,000 years to break by brute force. We really don't care how many zeroes there are on the end of that, as long as the number remains ridiculously large. That is, we don't care exactly how large the key is as long as it is large enough.

There may be reasons of convenience in the design of the cipher to support larger keys. For example Blowfish allows up to 448 bits and RC4 up to 2048, but beyond 100-odd bits it makes no difference to practical security.

CBC mode

Cipher Block Chaining mode , a method of using a block cipher in which for each block except the first, the result of the previous encryption is XORed into the new block before it is encrypted. CBC is the mode used in IPsec.

An initialisation vector (IV) must be provided. It is XORed into the first block before encryption. The IV need not be secret but should be different for each message and unpredictable.

Cipher Modes

Different ways of using a block cipher when encrypting multiple blocks.

Four standard modes were defined for DES in FIPS 81. They can actually be applied with any block cipher.

ECB	Electronic CodeBook	encrypt each block independently
CBC	Cipher Block Chaining	XOR previous block ciphertext into new block plaintext before encrypting new block
CFB	Cipher FeedBack	
OFB	Output FeedBack	

IPsec uses CBC mode since this is only marginally slower than ECB and is more secure. In ECB mode the same plaintext always encrypts to the same ciphertext, unless the key is changed. In CBC mode, this does not occur.

Various other modes are also possible, but none of them are used in IPsec.

Ciphertext

The encrypted output of a cipher, as opposed to the unencrypted plaintext input.

Client

This term has at least two distinct uses in discussing IPsec:

· The clients of an IPsec gateway are the machines it protects, typically on one or more subnets behind the gateway. In this usage, all the machines on an office network are clients of that office's IPsec gateway. Laptop or home machines connecting to the office, however, are not clients of that gateway. They are remote gateways, running the other end of an IPsec connection. Each of them is also its own client.

· IPsec client software is used to describe software which runs on various standalone machines to let them connect to IPsec networks. In this usage, a laptop or home machine connecting to the office is a client machine.

We generally use the term in the first sense. Vendors of Windows IPsec solutions often use it in the second.

Denial of service (DoS) attack

An attack that aims at denying some service to legitimate users of a system, rather than providing a service to the attacker.

· One variant is a flooding attack, overwhelming the system with too many packets, to much email, or whatever.

· A closely related variant is a resource exhaustion attack. For example, consider a "TCP SYN flood" attack. Setting up a TCP connection involves a three-packet exchange:

- Initiator: Connection please (SYN)
- Responder: OK (ACK)
- Initiator: OK here too

If the attacker puts bogus source information in the first packet, such that the second is never delivered, the responder may wait a long time for the third to come back. If responder has already allocated memory for the connection data structures, and if many of these bogus packets arrive, the responder may run out of memory.

· Another variant is to feed the system undigestible data, hoping to make it sick. For example, IP packets are limited in size to 64K bytes and a fragment carries information on where it starts within that 64K and how long it is. The "ping of death" delivers fragments that say, for example, that they start at 60K and are 20K long. Attempting to re-assemble these without checking for overflow can be fatal.

The two example attacks discussed were both quite effective when first discovered, capable of crashing or disabling many operating systems. They were also well-publicised, and today far fewer systems are vulnerable to them.

DES

The Data Encryption Standard, a block cipher with 64-bit blocks and a 56-bit key. Probably the most widely used symmetric cipher ever devised. DES has been a US government standard for their own use (only for unclassified data), and for some regulated industries such as banking, since the late 70's.

DES is seriously insecure against current attacks.

DH
see Diffie-Hellman

Diffie-Hellman (DH) key exchange protocol

A protocol that allows two parties without any initial shared secret to create one in a manner immune to eavesdropping. Once they have done this, they can communicate privately by using that shared secret as a key for a block cipher or as the basis for key exchange.

The protocol is secure against all passive attacks, but it is not at all resistant to active man-in-the-middle attacks. If a third party can impersonate Bob to Alice and vice versa, then no useful secret can be created. Authentication of the participants is a prerequisite for safe Diffie-Hellman key exchange. IPsec can use any of several authenticication mechanisims. Those supported by FreeS/WAN are discussed in our configuration section.

The Diffie-Hellman key exchange is based on the discrete logarithm problem and is secure unless someone finds an efficient solution to that problem.

Given a prime p and generator g (explained under discrete log below), Alice:

· generates a random number a
· calculates A = g^a modulo p
· sends A to Bob

Meanwhile Bob:

· generates a random number b
· calculates B = g^b modulo p
· sends B to Alice

Now Alice and Bob can both calculate the shared secret s = g^(ab). Alice knows a and B, so she calculates s = B^a. Bob knows A and b so he calculates s = A^b.

An eavesdropper will know p and g since these are made public, and can intercept A and B but, short of solving the discrete log problem, these do not let him or her discover the secret s.

Digital signature

Sender:

· calculates a message digest of a document
· encrypts the digest with his or her private key, using some public key cryptosystem.
· attaches the encrypted digest to the document as a signature

Receiver:

· calculates a digest of the document (not including the signature)
· decrypts the signature with the signer's public key
· verifies that the two results are identical

If the public-key system is secure and the verification succeeds, then the receiver knows

· that the document was not altered between signing and verification
· that the signer had access to the private key

Such an encrypted message digest can be treated as a signature since it cannot be created without both the document and the private key which only the sender should possess. The legal issues are complex, but several countries are moving in the direction of legal recognition for digital signatures.

EAR

The US government's Export Administration R egulations, administered by the Bureau of Export Administration. These have replaced the earlier ITAR regulations as the controls on export of cryptography.

EDE

The sequence of operations normally used in either the three-key variant of triple DES used in IPsec or the two-key variant used in some other systems.

The sequence is:

· Encrypt with key1
· Decrypt with key2
· Encrypt with key3

For the two-key version, key1=key3.

The "advantage" of this EDE order of operations is that it makes it simple to interoperate with older devices offering only single DES. Set key1=key2=key3 and you have the worst of both worlds, the overhead of triple DES with the security of single DES. Since single DES is insecure, this is an extremely dubious "advantage".

The EDE two-key variant can also interoperate with the EDE three-key variant used in IPsec; just set k1=k3.

Encryption

Techniques for converting a readable message (plaintext) into apparently random material (ciphertext) which cannot be read if intercepted. A key is required to read the message.
Major variants include symmetric encryption in which sender and receiver use the same secret key and public key methods in which the sender uses one of a matched pair of keys and the receiver uses the other. Many current systems, including IPsec, are hybrids combining the two techniques.

ESP

Encapsulated Security Payload, the IPsec protocol which provides encryption. It can also provide authentication service and may be used with null encryption (which we do not recommend). For details see our IPsec document and/or RFC 2406.

FIPS

Federal Information Processing S tandard, the US government's standards for products it buys. These are issued by NIST. Among other things, DES and SHA are defined in FIPS documents. NIST have a FIPS home page.

Hash

see message digest

Hashed Message Authentication Code (HMAC)

using keyed message digest functions to authenticate a message. This differs from other uses of these functions:
· In normal usage, the hash function's internal variable are initialised in some standard way. Anyone can reproduce the hash to check that the message has not been altered.
· For HMAC usage, you initialise the internal variables from the key. Only someone with the key can reproduce the hash. A successful check of the hash indicates not only that the message is unchanged but also that the creator knew the key.
The exact techniques used in IPsec are defined in RFC 2104. They are referred to as HMAC-MD5-96 and HMAC-SHA-96 because they output only 96 bits of the hash. This makes some attacks on the hash functions harder.

HMAC

see Hashed Message Authentication Code

HMAC-MD5-96

see Hashed Message Authentication Code

HMAC-SHA-96

see Hashed Message Authentication Code

ICMP

Internet Control M essage Protocol. This is used for various IP-connected devices to manage the network.

IDEA

International Data Encrypion Algorithm, developed in Europe as an alternative to exportable American ciphers such as DES which were too weak for serious use. IDEA is a block cipher using 64-bit blocks and 128-bit keys, and is used in products such as PGP.
IDEA is not required by the IPsec RFCs and not currently used in Linux FreeS/WAN.
IDEA is patented and, with strictly limited exceptions for personal use, using it requires a license from Ascom.

IKE

Internet Key Exchange, based on the Diffie-Hellman key exchange protocol.

Initialisation Vector (IV)

Some cipher modes, including the CBC mode which IPsec uses, require some extra data at the beginning. This data is called the initialisation vector. It need not be secret, but should be different for each message. Its function is to prevent messages which begin with the same text from encrypting to the same ciphertext. That might give an analyst an opening, so it is best prevented.

IP

Internet Protocol.

IPSec

Internet Protocol SECurity, security functions (authentication and encryption) implemented at the IP level of the protocol stack. It is optional for IPv4 and mandatory for IPv6.

ISAKMP

Internet Security Association and Key Management Protocol, defined in RFC 2408.

Man-in-the-middle attack

An active attack in which the attacker impersonates each of the legitimate players in a protocol to the other.
For example, if Alice and Bob are negotiating a key via the Diffie-Hellman key agreement, and are not using authentication to be certain they are talking to each other, then an attacker able to insert himself in the communication path can deceive both players.
Call the attacker Mallory. For Bob, he pretends to be Alice. For Alice, he pretends to be Bob. Two keys are then negotiated, Alice-to-Mallory and Bob-to-Mallory. Alice and Bob each think the key they have is Alice-to-Bob.
A message from Alice to Bob then goes to Mallory who decrypts it, reads it and/or saves a copy, re-encrypts using the Bob-to-Mallory key and sends it along to Bob. Bob decrypts successfully and sends a reply which Mallory decrypts, reads, re-encrypts and forwards to Alice.
To make this attack effective, Mallory must
· subvert some part of the network in some way that lets him carry out the deception
possible targets: DNS, router, Alice or Bob's machine, mail server, ...
· beat any authentication mechanism Alice and Bob use
strong authentication defeats the attack entirely; this is why IKE requires authentication
· work in real time, delivering messages without introducing a delay large enough to alert the victims
not hard if Alice and Bob are using email; quite difficult in some situations.
If he manages it, however, it is devastating. He not only gets to read all the messages; he can alter messages, inject his own, forge anything he likes, . . . In fact, he controls the communication completely.

Manual keying

An IPsec mode in which the keys are provided by the administrator. The alternative, automatic keying, is preferred in most cases.

MD4

Message Digest Algorithm Four from Ron Rivest of RSA. MD4 was widely used a few years ago, but is now considered obsolete. It has been replaced by its descendants MD5 and SHA.

MD5

Message Digest Algorithm Five from Ron Rivest of RSA, an improved variant of his MD4. Like MD4, it produces a 128-bit hash. For details see RFC 1321.
MD5 is one of two message digest algorithms available in IPsec. The other is SHA. SHA produces a longer hash and is therefore more resistant to birthday attacks, but this is not a concern for IPsec. The HMAC method used in IPsec is secure even if the underlying hash is not particularly strong against this attack.
Meet-in-the-middle attack
A divide-and-conquer attack which breaks a cipher into two parts, works against each separately, and compares results. Probably the best known example is an attack on double DES. This applies in principle to any pair of block ciphers, e.g. to an encryption system using, say, CAST-128 and Blowfish, but we will describe it for double DES.
Double DES encryption and decryption can be written:

C = E(k2,E(k1,P))
P = D(k1,D(k2,C))

Where C is ciphertext, P is plaintext, E is encryption, D is decryption, k1 is one key, and k2 is the other key. If we know a P, C pair, we can try and find the keys with a brute force attack, trying all possible k1, k2 pairs. Since each key is 56 bits, there are 2 112 such pairs and this attack is painfully inefficient.
The meet-in-the middle attack re-writes the equations to calculate a middle value M:

M = E(k1,P)
M = D(k2,C)

Now we can try some large number of D(k2,C) decryptions with various values of k2 and store the results in a table. Then start doing E(k1,P) encryptions, checking each result to see if it is in the table.
With enough table space, this breaks double DES with 256 + 256 = 257 work. Against triple DES, you need 256 + 2112 ~= 2112.
The memory requirements for such attacks can be prohibitive, but there is a whole body of research literature on methods of reducing them.
Message Digest Algorithm
An algorithm which takes a message as input and produces a hash or digest of it, a fixed-length set of bits which depend on the message contents in some highly complex manner. Design criteria include making it extremely difficult for anyone to counterfeit a digest or to change a message without altering its digest. One essential property is collision resistance. The main applications are in message authentication and digital signature schemes. Widely used algorithms include MD5 and SHA. In IPsec, message digests are used for HMAC authentication of packets.

NIST
The US National Institute of Standards and Technology, responsible for FIPS standards including DES and its replacement, AES.

Non-routable IP address
An IP address not normally allowed in the "to" or "from" IP address field header of IP packets.
Almost invariably, the phrase "non-routable address" means one of the addresses reserved by RFC 1918 for private networks:
· 10.anything
· 172.x.anything with 16 <= x <= 31
· 192.168.anything
These addresses are commonly used on private networks, e.g. behind a Linux machines doing IP masquerade. Machines within the private network can address each other with these addresses. All packets going outside that network, however, have these addresses replaced before they reach the Internet.
If any packets using these addresses do leak out, they do not go far. Most routers automatically discard all such packets.
Various other addresses -- the 127.0.0.0/8 block reserved for local use, 0.0.0.0, various broadcast and network addresses -- cannot be routed over the Internet, but are not normally included in the meaning when the phrase "non-routable address" is used.

Oakley
A key determination protocol, defined in RFC 2412.

Oakley groups
The groups used as the basis of Diffie-Hellman key exchange in the Oakley protocol, and in IKE. Four were defined in the original RFC, and a fifth has been added since.

One time pad
A cipher in which the key is:
· as long as the total set of messages to be enciphered
· absolutely random
· never re-used
Given those three conditions, it can easily be proved that the cipher is perfectly secure, in the sense that an attacker with intercepted message in hand has no better chance of guessing the message than an attacker who has not intercepted the message and only knows the message length. No such proof exists for any other cipher.
There are, however, several problems with this "perfect" cipher.
First, it is wildly impractical for most applications. Key management is at best difficult, often completely impossible.
Second, it is extremely fragile. Small changes which violate the conditions listed above do not just weaken the cipher a bit; quite often they destroy its security completely.
· Re-using the pad weakens it to the point where it can be broken with pencil and paper. With a computer, the attack is trivially easy.
· Using computer-generated pseudo-random numbers instead of a really random pad completely invalidates the security proof. Depending on random number generator used, this may also give an extremely weak cipher.
Marketing claims about the "unbreakable" security of various products which somewhat resemble one-time pads are common. Such claims are one of the surest signs of cryptographic snake oil. Systems marketed with such

claims are usually completely worthless.

Finally, even if the system is implemented and used correctly, it is highly vulnerable to certain types of attack. If an attacker knows the plaintext and has an intercepted message, he can discover the pad. This does not matter if the attacker is just a passive eavesdropper. It gives him no plaintext he didn't already know and we don't care that he learns a pad which we'll never re-use. However, knowing the pad lets an active attacker perform a man-in-the-middle attack, replacing your message with whatever he chooses.

Photuris
: Another key negotiation protocol, an alternative to IKE, described in RFCs 2522 and 2523.

PPTP
: Point-to-Point Tunneling Protocol. Papers discussing weaknesses in it are on counterpane.com.

PKI
: Public Key Infrastructure, the things an organisation or community needs to set up in order to make public key cryptographic technology a standard part of their operating procedures.
There are several PKI products on the market. Typically they use a hierarchy of Certification Authorities (CAs). Often they use LDAP access to X.509 directories to implement this.
Plaintext
The unencrypted input to a cipher, as opposed to the encrypted ciphertext output.

Public Key Cryptography
: In public key cryptography, keys are created in matched pairs. Encrypt with one half of a pair and only the matching other half can decrypt it. This contrasts with symmetric or secret key cryptography in which a single key known to both parties is used for both encryption and decryption.
One half of each pair, called the public key, is made public. The other half, called the private key, is kept secret. Messages can then be sent by anyone who knows the public key to the holder of the private key. Encrypt with the public key and you know only someone with the matching private key can decrypt.
Public key techniques can be used to create digital signatures and to deal with key management issues, perhaps the hardest part of effective deployment of symmetric ciphers. The resulting hybrid cryptosystems use public key methods to manage keys for symmetric ciphers.
Many organisations are currently creating PKIs, public key infrastructures to make these benefits widely available.

Public Key Infrastructure
: see PKI

RC4
: Rivest Cipher four, designed by Ron Rivest of RSA and widely used. Believed highly secure with adequate key length, but often implemented with inadequate key length to comply with export restrictions.

RC6
: Rivest Cipher six, RSA's AES candidate cipher.

Replay attack
: An attack in which the attacker records data and later replays it in an attempt to deceive the recipient.

RFC
: Request For Comments, an Internet document. Some RFCs are just informative

Routable IP address
: Most IP addresses can be used as "to" and "from" addresses in packet headers. These are the routable addresses; we expect routing to be possible for them. If we send a packet to one of them, we expect (in most cases; there are various complications) that it will be delivered if the address is in use and will cause an ICMP error packet to come back to us if not.
There are also several classes of non-routable IP addresses.

RSA algorithm

Rivest Shamir Adleman public key encryption method, named for its three inventors. The algorithm is widely used and likely to become moreso since it became free of patent encumbrances in September 2000.

For a full explanation of the algorithm, consult Applied Cryptography from B.Schneier. A simple explanation is:

The great 17th century French mathematician Fermat proved that, for any prime p and number x, 0 x^p == x modulo p x^(p-1) == 1 modulo p, non-zero x From this it follows that if we have a pair of primes p, q and two numbers e, d such that:

ed == 1 modulo lcm(p-1, q-1)

where lcm() is least common multiple, then for all x, 0 x^(ed-1) == 1 modulo pq, non-zero x x^ed == x modulo pq So we construct such as set of numbers p, q, e, d and publish the product N=pq and e as the public key. Encryption is then:

c = x^e modulo N

An attacker cannot deduce x from the cyphertext c, short of either factoring N or solving the discrete logarithm problem for this field. If p, q are large primes (hundreds or thousands of bits) no efficient solution to either problem is known.

The receiver, knowing the private key (N and d), can readily find x sixce:

c^d == (x^e)^d modulo N
== x^ed modulo N
== x modulo N

This gives an effective public key technique, with only a couple of problems. It uses a good deal of computer time, since calculations with large integers are not cheap, and there is no proof it is necessarily secure since noone has proven either factoring or discrete log cannot be done efficiently.

RSA Data Security

A company founded by the inventors of the RSA public key algorithm.

SA

Security Association, the channel negotiated by the higher levels of an IPsec implementation and used by the lower. SAs are unidirectional; you need a pair of them for two-way communication.

An SA is defined by three things -- the destination, the protocol (AH orESP) and the SPI , security parameters index. It is used to index other things such as session keys and initialization vectors.

For more detail, see our section on IPsec and/or RFC 2401.

Security Association

see SA

SHA

Secure Hash Algorithm, a message digest algorithm developed by the NSA for use in the Digital Signature standard, FIPS number 186 from NIST. SHA is an improved variant of MD4 producing a 160-bit hash.

SHA is one of two message digest algorithms available in IPsec. The other is MD5. Some people do not trust SHA because it was developed by the NSA. There is, as far as we know, no cryptographic evidence that SHA is untrustworthy, but this does not prevent that view from being strongly held.

SKIP

Simple Key management for Internet P rotocols, an alternative to IKE developed by Sun and being marketed by their Internet Commerce Group.

SPI

Security Parameter Index, an index used within IPsec to keep connections distinct. A Security Association (SA) is defined by destination, protocol and SPI. Without the SPI, two connections to the same gateway using the same protocol could not be distinguished.

For more detail, see our IPsec section and/or RFC 2401.

SSH

Secure SHell, an encrypting replacement for the insecure Berkeley commands whose names begin with "r" for "remote": rsh, rlogin, etc.

SSL

Secure Sockets Layer , a set of encryption and authentication services for web browsers, developed by Netscape. Widely used in Internet commerce. Also known as TLS.

Symmetric cryptography

Symmetric cryptography, also referred to as conventional or secret key cryptography, relies on a shared secret key, identical for sender and receiver. Sender encrypts with that key, receiver decrypts with it. The idea is that an eavesdropper without the key be unable to read the messages. There are two main types of symmetric cipher, block ciphers and stream ciphers.

Symmetric cryptography contrasts with public key or asymmetric systems where the two players use different keys.

The great difficulty in symmetric cryptography is, of course, key management. Sender and receiver must have identical keys and those keys must be kept secret from everyone else. Not too much of a problem if only two people are involved and they can conveniently meet privately or employ a trusted courier. Quite a problem, though, in other circumstances.

It gets much worse if there are many people. An application might be written to use only one key for communication among 100 people, for example, but there would be serious problems. Do you actually trust all of them that much? Do they trust each other that much? Should they? What is at risk if that key is compromised? How are you going to distribute that key to everyone without risking its secrecy? What do you do when one of them leaves the company? Will you even know?

On the other hand, if you need unique keys for every possible connection between a group of 100, then each user must have 99 keys. You need either 99*100/2 = 4950 secure key exchanges between users or a central authority that securely distributes 100 key packets, each with a different set of 99 keys.

Either of these is possible, though tricky, for 100 users. Either becomes an administrative nightmare for larger numbers. Moreover, keys must be changed regularly, so the problem of key distribution comes up again and again. If you use the same key for many messages then an attacker has more text to work with in an attempt to crack that key. Moreover, one successful crack will give him or her the text of all those messages.

In short, the hardest part of conventional cryptography is key management. Today the standard solution is to build a hybrid system using public key techniques to manage keys.

TLS

Transport Layer Security, a newer name for SSL.

Transport mode

An IPsec application in which the IPsec gateway is the destination of the protected packets, a machine acts as its own gateway. Contrast with tunnel mode.

Triple DES

see 3DES

Tunnel mode

An IPsec application in which an IPsec gateway provides protection for packets to and from other systems. Contrast with transport mode.

Two-key Triple DES

A variant of triple DES or 3DES in which only two keys are used. As in the three-key version, the order of operations is EDE or encrypt-decrypt-encrypt, but in the two-key variant the first and third keys are the same.

3DES with three keys has 3*56 = 168 bits of key but has only 112-bit strength against a meet-in-the-middle attack, so it is possible that the two key version is just as strong. Last I looked, this was an open question in the research literature.

RFC 2451 defines triple DES for IPsec as the three-key variant. The two-key variant should not be used and is not implemented directly in Linux FreeS/WAN. It cannot be used in automatically keyed mode without major fiddles in the source code.

Virtual Private Network

see VPN

VPN
: Virtual Private Network, a network which can safely be used as if it were private, even though some of its communication uses insecure connections. All traffic on those connections is encrypted.
IPsec is not the only technique available for building VPNs, but it is the only method defined by RFCs and supported by many vendors. VPNs are by no means the only thing you can do with IPsec, but they may be the most important application for many users.

Wassenaar Arrangement
: An international agreement restricting export of munitions and other tools of war. Unfortunately, cryptographic software is also restricted under the current version of the agreement. Discussion.

X.509
: A standard from the ITU (International Telecommunication Union), for hierarchical directories with authentication services, used in many PKI implementations.