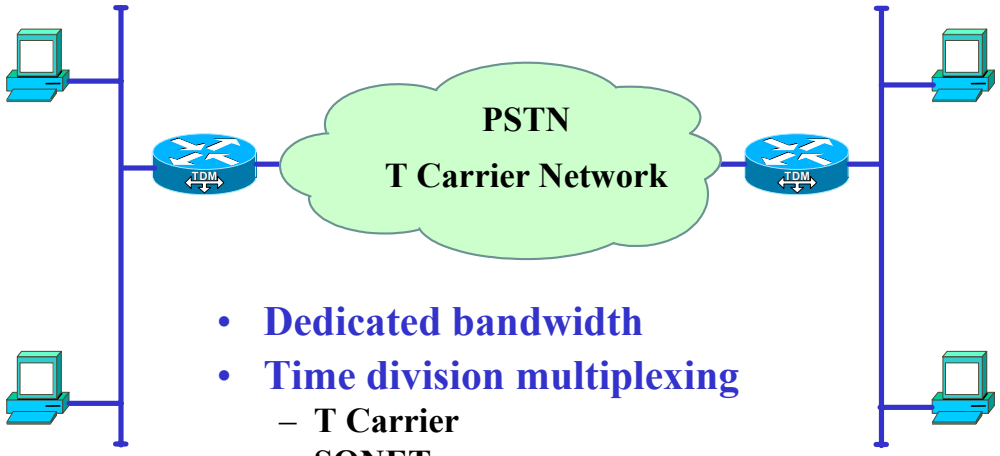
Bob's VPN Overview

An overview of VPN Concepts & Technology

VPN – Objectives

- Define the term "Virtual Private Network"
- Describe several VPN types and applications
- Explain tunneling benefits, features, & risks
- List 4 popular tunneling protocols & the environments in which they are found

Private Networks



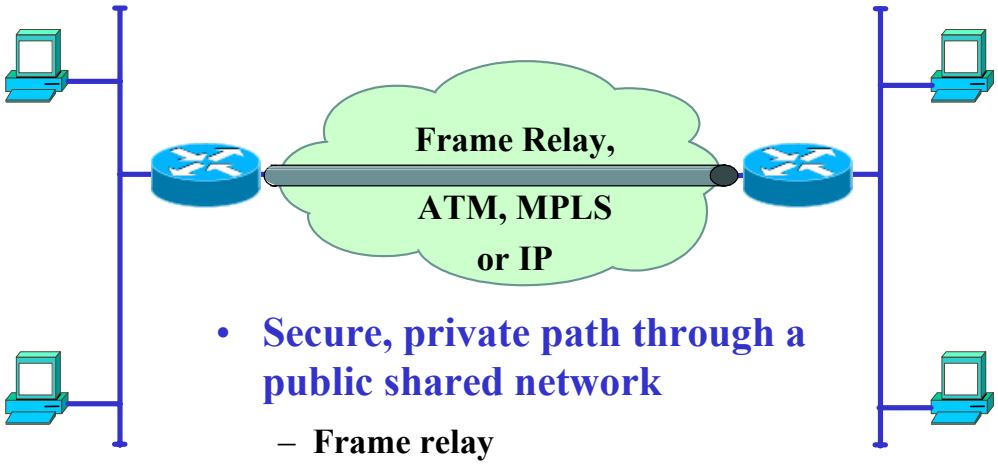
- Dedicated bandwidth
- Time division multiplexing
  - T Carrier
  - SONET
- Secure
- Expensive

Private Networks

Private networks can offer the most security. Unfortunately, they are also the most costly. Composed of privately owned and operated switches or routers interconnected with dedicated private line services, private networks are deployed where traffic flows warrant or security demands require (such as those at various 3-lettered government agencies). Most businesses strive to find less expensive alternatives that meet their performance and security expectations.

Private network transmission costs are the real budget breaker. Dedicated private lines are priced upon the throughput in Mbps and the distance between sites. The greater the link speed, number of sites, and distance between them, the higher the cost. Monthly recurring transmission costs can consume as much as 85% of the annual IT budget in large nationwide private topologies. Private network transmission technologies commonly deployed over the years include analog "3002-grade" lines, DDS, T-1 and Fractional-T, DS-3 and fractional, SONET, and various other fiber-based services.

Virtual Private Networks



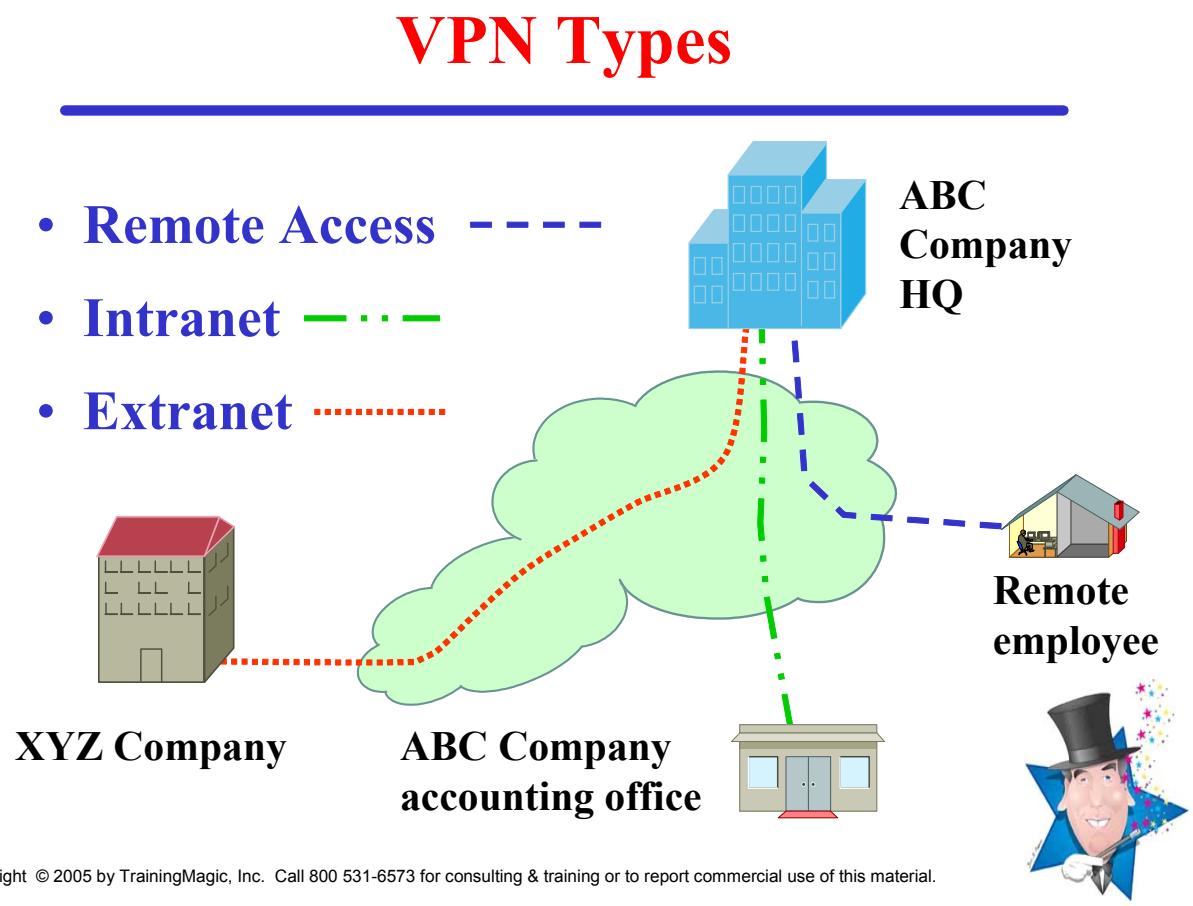
- **Secure, private path through a public shared network**
  - **Frame relay**
  - **ATM**
  - **MPLS**
  - **IP**

Virtual Private Networks

Virtual: Existing in essence or effect though not in actual fact…
- American Heritage Dictionary

A Virtual Private Network, or VPN, describes a network service where the illusion of a dedicated private connection is provided to the user, but in reality is not. VPN services inherently share transmission facilities and switching functions among multiple end users. This implies that network services may temporarily unavailable for one users transfer request while another customer's information transfer is serviced. But by sharing the cost of network deployment across many users, the individual cost per user can be very low compared to a dedicated network. Couple the cost benefit with the fact that many transfers don't require instantaneous delivery and you can see why shared VPN services are so attractive.

Two major concerns arise when using Virtual Private Network services: Performance and Security. Performance can be quantified using multiple metrics including throughput, error rate, latency, availability, MTBF, MTTR, and more. Because the shared network service carries traffic originating from different customers, a second worry arises: Can other network users intercept or compromise my data? Obviously, few would subscribe to a service that answered yes to that question. All successful VPN services including Frame Relay, ATM, MPLS, and IP-based, have provided means for ensuring privacy. In IP-based VPN's, this is usually accomplished by the use of encryption and tunneling protocols.



VPN Types

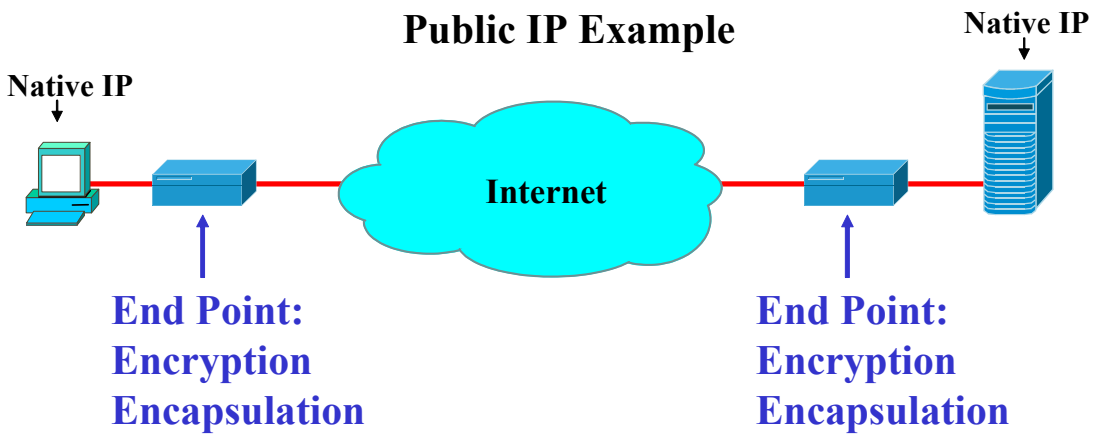
VPN topologies are often categorized by the applications they serve: Remote Access, Intranet, and Extranet.

Remote Access VPN's are frequently used in lieu of a direct dialup connection between a single remote user and a corporate site. For security, IP-based Remote Access VPN's may either rely upon software deployed on the remote client or upon a service provider's Network Access Server (NAS) to encapsulate and forward traffic to a corporate site. Remote Access VPN's can reduce long distance dial charges and offer higher throughputs than direct dial.

Intranet VPN solutions interconnect multiple sites belonging to the same company. The distinction between Intranet and Remote Access is based primarily on the number of users. Remote Access VPN's are geared toward allowing a single remote user access to informational resources located at "headquarters." Intranet VPN solutions are designed to support multiple users accessing information located at either HQ or the other office locations. As technologies such as DSL, Cable, and bi-directional satellite bring high-speed connectivity to home LANs, the distinction between Remote Access and Intranet VPN's can often become blurred.

Extranet VPN's are designed to foster sharing of information between companies. There are numerous applications labeled as "extranet" today. Order entry, order status, electronic payment, browsing inventory, electronic data interchange (EDI) are all candidate applications for the extranet. The crucial distinction here is that information is being securely passed between members of different companies. As a business extranet operator, you strive to ensure that your business partners can access appropriate information they need, but can't access more than that!

IP-based VPNs



IP-based VPN's

IP-based VPN's utilize an IP router backbone for traffic carriage. Many immediately think of the Internet when discussing an IP backbone, but other IP-based networks clearly apply. While low cost DSL and Cable Modem connections are an attractive access to the greater Internet, little can be guaranteed when discussing the Internet and Quality or Availability of service. Instead, many service providers make available separate IP facilities or prioritized services for their higher-paying VPN customers.

To provide security in VPN applications, data is typically encrypted and encapsulated before traversing a public IP service. A logical connection is established between devices on either side of the public IP network prior to sending data. This logical connection, or virtual circuit, is frequently called a “tunnel”. The devices at each end of the tunnel, called tunnel endpoints, are responsible for encrypting, sequencing, and encapsulating data before transmitting over the IP backbone. A tunnel endpoint may be physically located in a client, a server, a router or firewall with appropriate software added, or purpose-built devices known as VPN concentrators.

.

Tunneling: A Definition

- **A technique that enables one network to transmit its data via another network's connectivity**
- **Frequently compared with Encapsulation**

Usually encrypted

Tunneling: A Definition

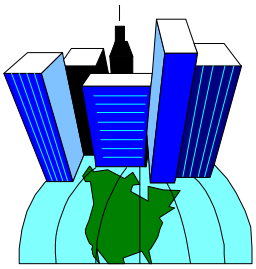
Tunneling is a technique that enables one network to send its data via another network's connectivity. Tunneling works by encapsulating one network's protocol within data units carried by the second network.

Tunneling is also called *encapsulation*; a comparison that has sparked heated debate over the years. The argument distinguishing Tunneling from Encapsulation is related to duplicate OSI layering. But the basic concept in each case is the same: Take a packet or frame from one network and place it as the payload inside another network's packet or frame.

This onion layering is not without overhead. Tunneled solutions always incur additional transmission overhead and processing overhead at the tunnel endpoints. The amount varies by tunneling protocol and function.

IP Tunneling Benefits

- $ave Money ?
- Use existing, ubiquitous IP networks
- Multiprotocol Support
- Privacy, Security, Authenticity



IP Tunneling Benefits

The potential to save big coin tempts many to investigate VPN solutions. When compared to deploying private dedicated lines, VPN costs can be very attractive. But remember that data sent over private lines is typically not encrypted – it's considered secure because the lines are private. Just the opposite is the norm in IP VPN's: In all but the simplest applications, encryption is mandatory. This encryption at each tunnel endpoint requires processing power so not to impinge on network throughput, and the costs begin to escalate… The more secure, the higher the cost.

With IP networks now deployed within most corporations, and public ISP networks spanning the globe (with even a few nodes now in space!), taking advantage of the existing connectivity only makes sense. Unfortunately for some, IP networks only carry IP. But that doesn't mean that organizations using protocols other than IP are "out of luck." IP Tunneling protocols can transport just about any protocol you can think of. Shunting Novell IPX or AppleTalk traffic between corporate sites via an IP-only backbone has been a popular solution until those architectures embraced IP natively. Data Link Switching (DLSw) has been used for years to project IBM's Systems Network Architecture (SNA) traffic atop an IP backbone.

But most importantly, tunneling protocols add security to an architecture, which has traditionally lacked it. The Internet Protocol Suite was initially designed for an open cooperative educational and research forum. Communications between multi-vendor systems was the goal, not secrecy. However, if sensitive information is to traverse IP networks, such as that in E-business or E-commerce, ensuring the authenticity and privacy of transmissions is vital.

Tunneling Features

- **Endpoint Identity, Authenticity**

- **Data Integrity**

- **Data Confidentiality**

Tunneling Features

Tunneling protocols can provide a variety of features, some optional, others mandatory, depending on the application and specific protocol. Among them are:

Mutual Authentication: Prior to, or during, tunnel establishment, the tunnel endpoint identities are established and confirmed unambiguously. This can be done using a combination of keys or passwords, IP addresses, digital signatures, and certificates.

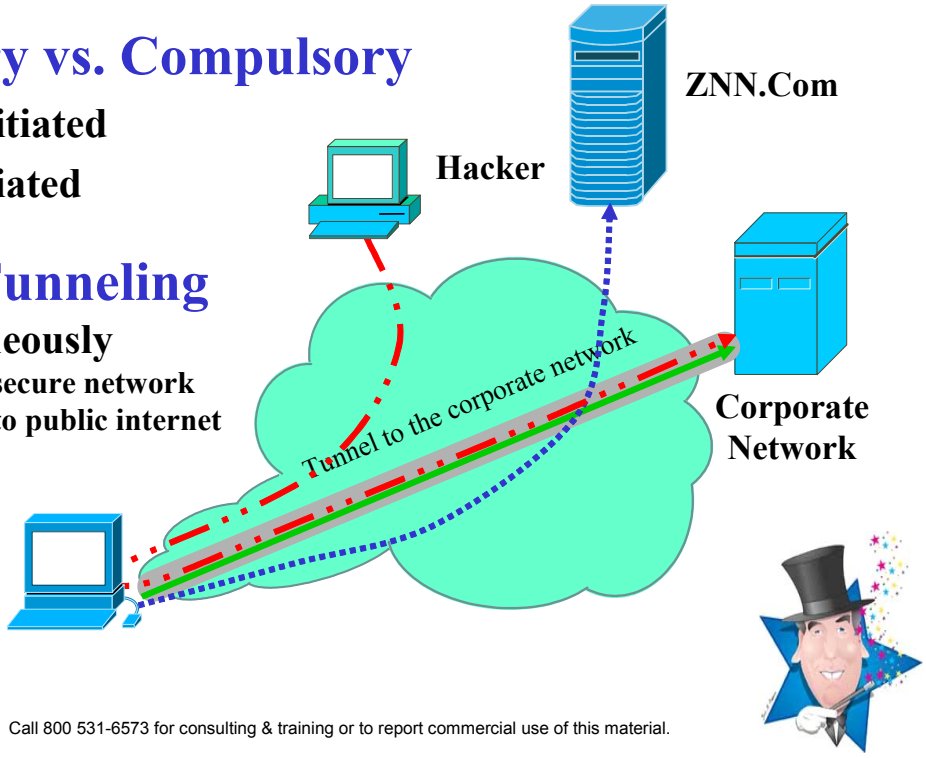
Data Encryption: To ensure the privacy of information traversing the tunnel, endpoints will encrypt data prior to transmission. A variety of encryption techniques may be employed including DES, 3DES, AES, and others. Some tunneling protocols are capable of negotiating the encryption method and dynamically selecting session keys that are changed periodically.

Data Integrity: Hash functions are generally used to detect transmissions that have been tampered with during transmission.
Data Compression: Higher throughputs can be achieved by first compressing data prior to encryption and transmission. This feature is optional in many protocols.

Protocol Identification: Some tunneling methods, such as PPTP and GRE, are capable of carrying numerous protocol payload types over the same tunnel. In these cases, a protocol identifier within the encapsulation header is vital for receiver processing.

Tunneling Terms

- **Voluntary vs. Compulsory**
  - **Client initiated**
  - **NAS initiated**
- **"Split" Tunneling**
  - **Simultaneously**
    - **Access secure network**
    - **Access to public internet**
  - **Risky**



Tunneling Terms

Voluntary tunnels are optional: the user has the option of creating or not creating the tunnel. Voluntary tunnels are most often found in the context of Client-initiated VPN's where the End-user controls and maintains both tunnel endpoints. The Service provider in this case provides only basic transport.

Compulsory tunnels are not optional: user data must travel via the tunnel or not at all. This operation is typical of Network Access Server (NAS) initiated VPN services. The Service Provider's NAS establishes the necessary tunnel on behalf of the calling remote user to the corporate network. These arrangements require coordination between service provider and the corporate user.

A tunnel is said to be "split" if a remote user or site can send traffic via the secure tunnel and via an alternate Internet access at the same time. While such arrangements can offer performance advantages for the remote user, a serious security issue is raised. If the remote user is hacked from their alternate Internet connection, the compromised remote device acts as a secure conduit via the VPN into the corporate intranet! Firewall functions on the remote user can reduce this risk, but frequently corporate security policies simply forbid split tunnels to be safe.

IP Tunneling Protocols

Most common

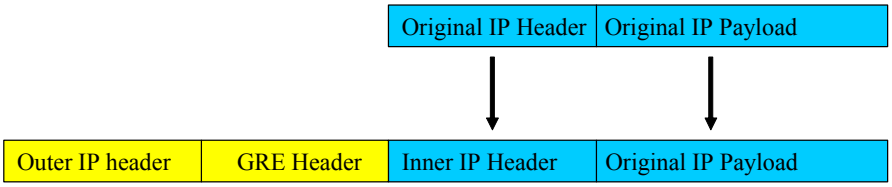
	PPTP	L2F	L2TP	IPSec
Multiple users per tunnel	No*	Yes	Yes	Yes
Sponsor	Microsoft, PPTP Forum	Cisco	IETF	IETF
Data Encap. Type (typical)	IP/GRE	L2F/UDP	L2TP/UDP	IP/GRE
Encryption	MPPE	MPPE	MPPE or IPSec	IPSec

IP Tunneling Protocols

There are a number of tunneling protocols popular in contemporary VPN applications. This matrix categorizes several protocols with respect to sponsor or standard, typical data encapsulation layering, encryption options, and support for multiple independent data streams or users.

GRE

- **Generic Routing Encapsulation, RFC-1701, 1702**
- **Simple Router-to-Router Intranet VPN solution**
- **Support for IP and other network layer protocols**



IP in GRC example

GRE

Generic Routing Encapsulation was developed in 1994 in an effort to standardize attempts at carrying non-IP traffic atop Internet facilities. GRE's primary function is to identify the protocol being carried by defining a protocol type field in its header similar to Xerox Ethernet EtherType values or IEEE 802.2 SNAP headers.

Terminology in GRE describes a Passenger Protocol, Carrier Protocol, and Transport Protocol. The passenger protocol is that being transported by encapsulation. The carrier protocol is simply the GRE envelope that describes the encapsulated contents. The transport protocol, usually IP, is the encapsulating protocol, which moves both the passenger and carrier protocols over some backbone.

The GRE header contains a small number of mandatory fields including GRE "Version" number (currently 0) and "Protocol" (identifies the passenger protocol type). This header is then typically encapsulated within an IP packet addressed to the distant GRE tunnel endpoint.

Optional fields may be included for additional functionality. The optional "Key" field contains a 32-bit number inserted by the sending tunnel endpoint to authenticate the packet source. Because the GRE header and this number are in plaintext form, the Key could be easily intercepted and emulated. The optional "Sequence Number" field contains a 32-bit number inserted by the transmitter to identify the sequence in which packets have been transmitted. While the sequence numbering would obviously be compromised were a hacker to attempt data insertion, the receiver has only the key and source IP address to determine valid data from bogus hacking. An optional "Route" field may be employed to contain a list of source route entries. When the route field is used, an optional "Offset" field is added to indicate the variable length, which route entries may entail.

GRE by itself offers little in the way of true security. Recall that it's primary purpose was in support of protocol identification. That is not to say that GRE has no use in secure tunneling applications. Instead, it's multiprotocol capabilities are sometimes used in conjunction with IPsec by Cisco products.

GRE Example

- **Cisco IOS GRE configuration**

```
interface Tunnel0
! Tunnel interface 0
 ip address 192.168.20.1 255.255.255.0
! Ip address of the gre tunnel interface 0
 tunnel source Ethernet0
! Ip source of the tunnel. It's best to make this an
! interface with a public, routable IP address so that
! it's reachable from the other endpoint of the tunnel.
 tunnel destination 11.11.11.11
! Ip destination of the tunnel. Make sure this is
! reachable via the "ping" command otherwise the
! tunnel will not be created properly.
!
```

GRE Example

Many vendors for tunneling both IP and other protocols over an IP backbone support GRE. Of almost all current tunneling protocols, GRE burdens routers the least with processing effort. That's primarily because GRE (by itself) does not include requirements for encryption. GRE's primary function is to identify the payload type being carried. So what of security? GRE supports several features, which by coincidence could reject would-be hackers from inserting their own data into existing tunnels or establishing their own tunnels.

Tunnel Source & Destination:
Tunnel Key:
Sequence numbers:

PPP

- **Point-to-Point Protocol, RFC-1661**
- **Data Link protocol: Dialup, Dedicated Line,…**
- **Sub-prototcols for: Authentication, Address assignment, Compression, Encryption, more…**

IP in PPP example

PPP

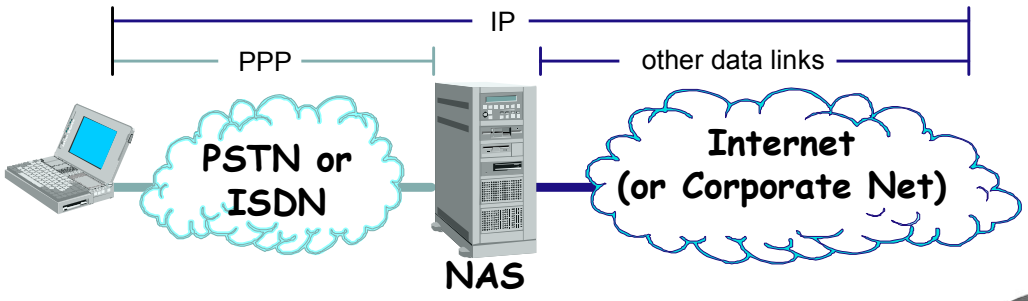
The Point-to-Point Protocol is now the most widely deployed Remote Access data link protocol to date. PPP is derived from ISO HDLC principles and shares a similar header/trailer structure. PPP may be deployed atop dedicated lines such as DS-1 or SONET, or over dialup connections such as POTS or ISDN. Over the years, PPP has been adapted for use in other technologies such as DSL.

The primary purposes of PPP are to delimit packets, detect transmission errors, and identify encapsulated payloads. PPP defines a number of ancillary protocols, which add a wealth of optional features. Some of the more important protocols are:

PAP: Password Authentication Protocol – simple plaintext exchange of username/password credentials
CHAP: Challenge Handshake Authentication Protocol – encrypted exchange of username/password credentials
LCP: Link Control Protocol – Configures specific layer 2 operational parameters
CCP: Compression Control Protocol – negotiates data stream compression parameters
IPCP: Internet Protocol Control Protocol – dynamically assigns IP parameters (IP address, mask, gateway, DNS)

PPP Dialup Topology

- **Data Link between Client & NAS**



PPP Dialup Topology

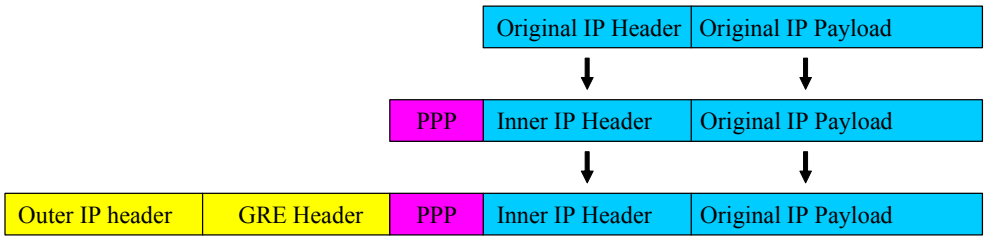
In Dialup scenarios, the Point-to-Point Protocol (PPP) is used on the physical link between a dialup client and its Network Access Server (NAS) to detect transmission errors and identify encapsulated protocols. Transmissions from either device, such as IP packets, are encapsulated within PPP frames and sent to the other end. Receivers can discern if transmission errors have occurred using PPP's Cyclic Redundancy Check (CRC) trailer. They may also determine the encapsulated payload type (IP, ARP, IPX, other) by the Protocol ID field within PPP's header.

In a typical ISP dialup scenario, or in a typical Corporate Dialup RAS scenario, the Access Server strips away the PPP framing, and forwards only the contained payload. This routing function in the NAS encapsulates the denuded payload within a new frame (Ethernet, Frame Relay, FDDI, etc.) depending upon the next-hop technology. In these scenarios, PPP lives up to its name well: It is Point-to-Point only. But this being the case, requires that a physical channel extend from the client directly to the NAS. If these are located far from each other, long distance dial charges could become a major concern.

But it's PPP's ancillary protocols that really shine in the dialup scenario. Remember that frequently dialup users are unfamiliar with TCP/IP protocols and configuration specifics. It's PPP that comes to their rescue. LCP dynamically negotiates link parameters. PAP or CHAP identify and authenticate the user allowing the ISP to record usage times and other accounting details. IPCP automatically assigns IP address, network masks, DNS, and other settings for that session. Were it not for PPP's auto-configuration capabilities, far fewer people would be surfing the net today!

PPTP

- **Point-to-Point Tunneling Protocol, RFC-2637**
- **Most widely used Remote Access VPN protocol**



IP in PPTP example

PPTP

As Internet Service Providers began to blanket the country with dial access points in the early and mid 1990's, many Corporations and ISPs began to wonder if that infrastructure might be used to supplant the separate, parallel dial facilities being deployed for remote corporate network access. In essence, the ISP could provide the connectivity for a Virtual Private Dialup Network, or VPDN. Two major vendors each brought forth solutions: Cisco with their Layer 2 Forwarding (L2F), and Microsoft with their Point-to-Point Tunneling Protocol (PPTP).

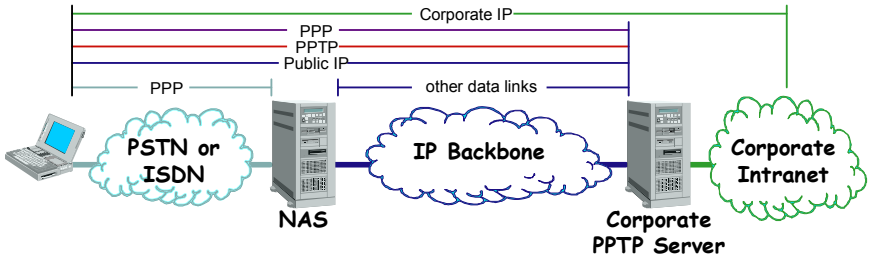
The Point-to-Point Tunneling Protocol has been the most widely deployed Remote Access VPN protocol to date primarily because of its integration with all Microsoft desktop operating system products since Windows 95 OSR2*. This protocol was initially developed to provide Virtual Private Dialup Network (VPDN) capabilities in late 1995 by the PPTP Forum (Ascend, Microsoft, USRobotics, 3Com, Copper Mtn, and ECI Telematics.) The PPTP Forum's "generic" protocol description was later accepted by the IETF as RFC-2637. However, it is instead Microsoft's PPTP implementation that virtually all vendors comply with because of Microsoft's market penetration.

Microsoft has laden their PPTP implementation with several proprietary extensions to the PPTP Forum specification. (Surprise!) Microsoft PPTP defaults to MS-CHAP (Microsoft - Challenge Handshake Authentication Protocol) for authentication. Two versions of this (v1 and v2) now exist following the discovery of significant weaknesses in the earlier MS-CHAPv1. Options for PAP, CHAP, and SPAP are manually selectable in Microsoft's PPTP setup.

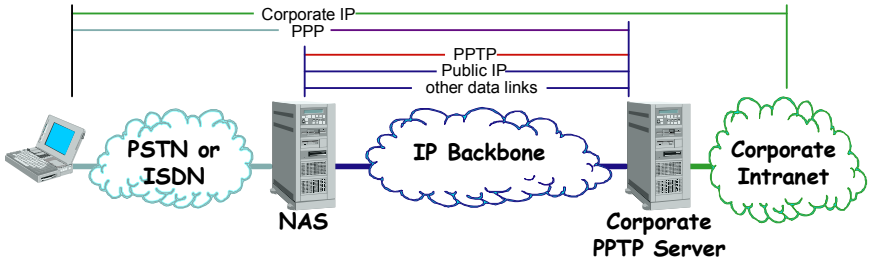
Microsoft Point-to-Point Encryption (MPPE) is used for data encryption (which is mandatory by default.) This encryption preference is indicated within Microsoft's Compression Control Protocol (CCP) implementation used during PPP negotiation as the tunnel is established. (By default, data is also compressed prior to encryption.) MPPE employs RSA's RC4 algorithm to create a continuous stream of random bytes based upon an initial seed; an encryption key. This stream is then XORed (eXclusive OR) with the data stream to create cipher text sent to the receiver. The receiver applies an XOR operation to the received cipher text with a locally generated RC4 stream based on the same encryption key.** The 40-bit (export) or 128-bit (domestic) session encryption key, is derived from the Windows credentials known by both the sender and receiver and confirmed during the authentication phase. While this is an elegant solution to the age-old key distribution problem, therein lies a weakness to MPPE's security: The encryption is only as secure as your username/password combination!

* OSR2: Original-Equipment-Manufacturers (OEM) Service Release 2.
** Adapted from http://www.win2000mag.com/Articles/Index.cfm?ArticleID=5188 and
http://www.microsoft.com/ntserver/ProductInfo/faqs/PPTPfaq.asp

PPTP Topologies



PPTP-enabled Client example



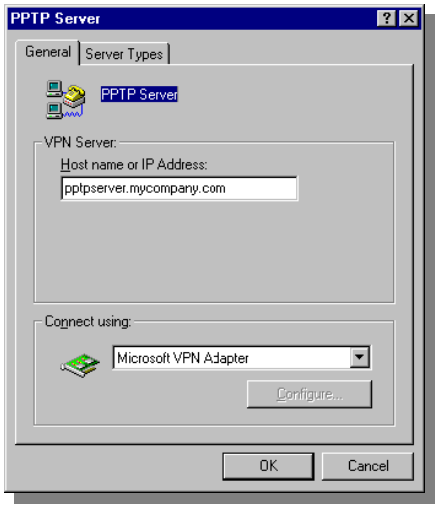
PPTP-enabled NAS example

PPTP Topologies

PPTP allows a PPP session to be extended over an IP backbone to a corporate PPTP server. This can eliminate long distance dial charges and shift requirements for modems and POTS lines to the ISP. The end result gives remote users access to corporate networks without the need to deploy a corporate dial infrastructure. PPTP may be deployed in two primary topologies depending upon the ISP/carrier's support for PPTP. In one case, the client itself houses the originating tunnel endpoint. In the other, the carrier's NAS houses the originating tunnel endpoint.

PPTP Example

- **PPTP client built into all Windows NT/2000/XP**
- **Connects to PPTP RAS**

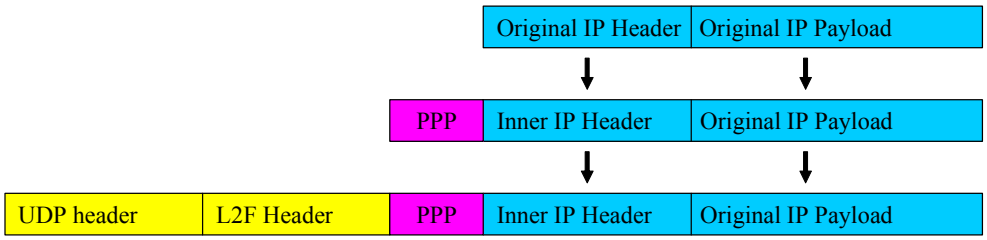


PPTP Client

Windows NT/2000/XP has a built in PPTP Remote Access Server (RAS) client. Windows PPTP allows a computer to establish a private tunnel over a "public" IP backbone and connect to a RAS that supports PPTP.

L2F

- **Layer 2 Forwarding, RFC-2341, historic**
- **Cisco (early) VPDN tunneling protocol**



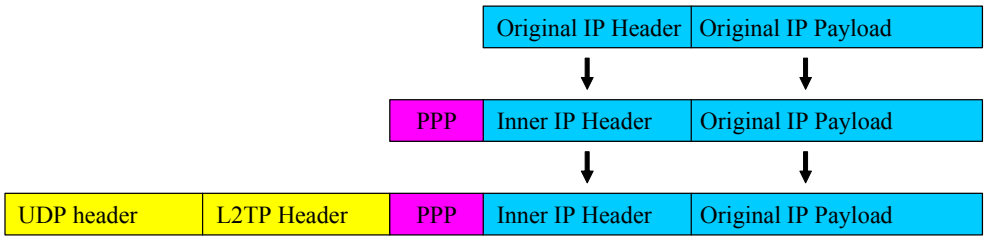
IP in L2F example

L2F

Layer 2 Forwarding was devised by Cisco to encapsulate and carry SLIP or PPP frames from a Service Provider's dialup Network Access Server to a corporate network. This allows Service Providers to provide a Virtual Private Dialup Network (VPDN) service to the Enterprise user and allow corporates to avoid installing and maintaining their own dial servers and connectivity in remote areas. L2F can carry encapsulated traffic using a variety of transport technologies including Frame Relay, ATM, and IP backbones. A single L2F tunnel can carry multiple logical streams or user traffic as distinguished by its *Multiplex ID* and *Client ID* fields. While the protocol is still deployed in rare instances, Cisco no longer advocates its use, preferring instead a newer hybrid, which combines aspects of L2F with PPTP. That newer protocol is the Layer 2 Tunneling Protocol, or L2TP.

L2TP

- **Layer 2 Tunneling Protocol, RFC-2661**
- **Combines PPTP & L2F Features**



IP in L2TP example

L2TP

The Layer 2 Tunneling Protocol (L2TP) described in IETF RFC-2661 (STD-51), combines aspects of both L2F and PPTP implementations. And with both Cisco and Microsoft behind it, you would suspect heavy penetration into the VPN world. Unfortunately, numerous implementation options have frustrated cross-vendor implementations until recently. Securing L2TP using IPsec has been put forth as an IETF proposed standard under RFC-3193 and implemented by Microsoft in its Windows 2000 and XP operating systems. Standards for transporting L2TP atop Frame Relay have even been defined.

The L2TP protocol's PPP heritage brings much to the client-initiated, voluntary VPN: Authentication procedures, address assignment, and traditional PPP extensions included. Its support in NAS-initiated compulsory tunnel applications is fostered by Cisco with proposed standards under RFC-2809.

IPsec Overview

- **Originally defined/mandated for IPv6**
- **Three Main Components**
  - **Authentication Header (AH)**
  - **Encapsulating Security Payload (ESP)**
  - **Internet Key Exchange (IKE)**

IPsec Overview

The Internet Protocol Suite was originally devised to facilitate communications between different manufacturer's computer systems. Secrecy was simply not an original design goal. As a result, IP packets have no innate security. It is fairly easy to spoof the source address in IP packets, change the contents of IP packets, inspect the contents of IP packets in transit, and to capture IP packets and replay them at a later time. This means that there is no inherent guarantee that received IP packets are from the claimed sender, contain the originally transmitted data, or have not been read by a third party in transit.

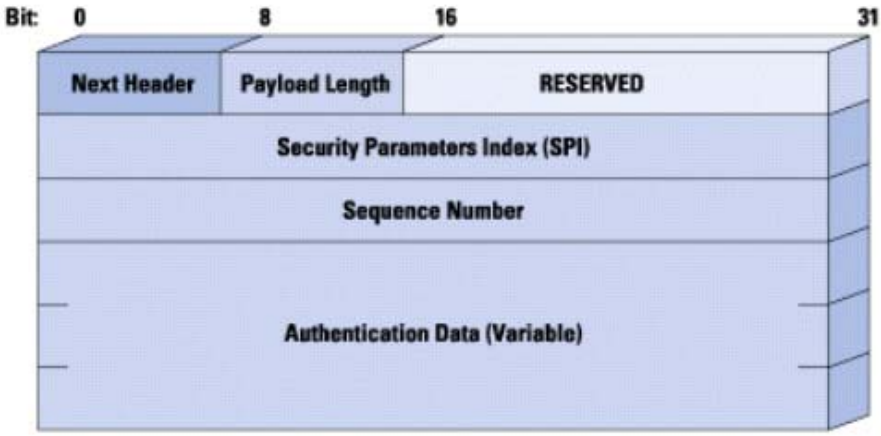
IPsec is a standard method for securing IP packets. Having originally been designed for IPv6, implementations are now standardized and integrated into many IPv4 systems. IPsec's protections include data origin authentication, data integrity assurance, data confidentiality, and anti-replay protection. IPsec can operate in "transport mode" where only the upper-layer information is protected. Or IPsec may run in "tunnel mode" where an entire IP datagram is secured then encapsulated in a second IP packet for transmission.

There are three main components to the IPsec architecture described in RFC-2401. The Authentication Header (AH) protocol provides proof of data origin, data integrity, and anti-replay protection (but not confidentiality.) The Encapsulating Security Payload (ESP) protocol provides all that AH does but adds data confidentiality and limited traffic flow confidentiality options. IPsec allows systems to use a variety of cryptographic algorithms as agreed to by endpoints. Today's implementations commonly use DES and 3DES, but other encryptions are available and deployed.

The set of tunneling parameters to be used when sending traffic from one device to another is called a "Security Association." Parameters such as crypto method, encapsulation options, and encryption keys, must be established prior to data transmission. Some of these parameters may be statically configured in the IPsec devices or be distributed via the Internet Key Exchange or IKE.

Authentication Header (AH)

- **Assures: origin, integrity, anti-replay**

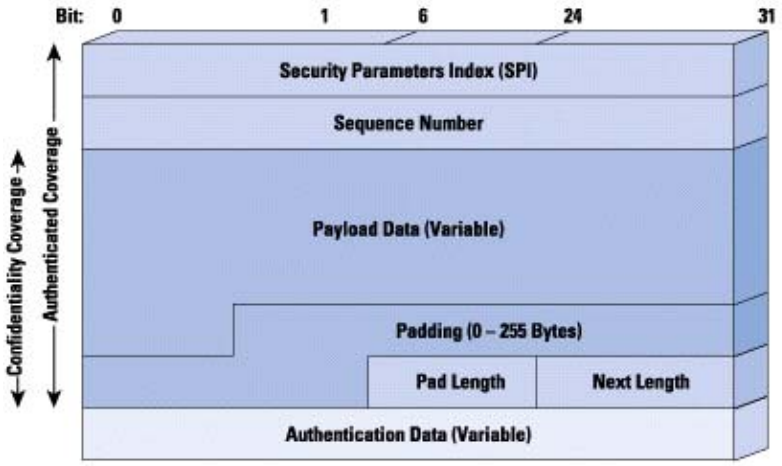


Authentication Header

The Authentication Header (AH) protocol, specified in RFC-2402, is used to assure data origin (authenticity), data integrity, and anti-replay, but not data confidentiality. The AH contains a message authentication code (authentication data) that is calculated using a key and hash function defined in the security association already established between the two parties. Because some of the IP header fields will change during transit, only the static header fields are processed. If confidentiality is desired, the AH can be used in conjunction with the Encapsulating Security Payload (ESP) protocol. The AH protocol can operate in “transport” mode, where the end system IP address and header information is used for end-to-end transmission. AH may also operate in “tunnel” mode where the entire originating IP packet is encapsulated within another IP packet header. Tunnel mode is an obvious solution where end systems are using RFC-1918 private IP addresses yet wish to connect atop the public Internet. Remember though, that the payloads in either case remain unencrypted and readable if intercepted.

Encapsulating Security Payload (ESP)

- **Assures: origin, integrity, anti-replay, confidentiality, data flow confidentiality**

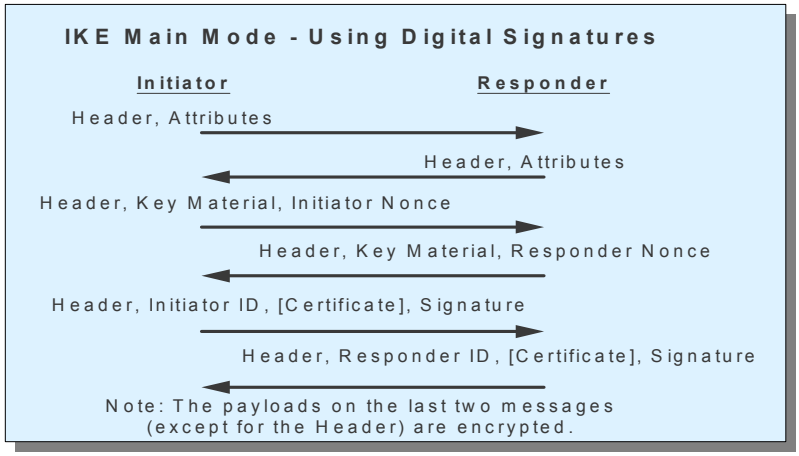


Encapsulating Security Payload

The Encapsulating Security Payload (ESP) protocol, specified in RFC-2406, provides all the data assurances assumed by the Authentication Header (AH) protocol, including data origin (authenticity), data integrity, and anti-replay. But in addition to these services, ESP can provide data confidentiality (encryption) and limited data flow confidentiality. Because ESP provides both authentication and confidentiality, it defines multiple algorithms in its SA: one for authentication called the authenticator, a second for confidentiality called a cipher. All encryption methods used by ESP must perform cipher block chaining (CBC). CBC requires that the amount of encrypted data be an integral multiple of the cipher block size. Padding is placed at the end of the data prior to encryption in order to meet this constraint. The ESP header is left in plaintext so that the receiver may use the Security Parameters Index along with the source IP address to select and apply the proper SA. A sequence number is used to assist in anti-replay detection. The authentication data which follows the encrypted payload contains a hash result performed on the payload plus padding and length fields. MD5 and SHA are specified as authenticator algorithms. ESP does not strictly stipulate what ciphers are to be used, but rather imposes certain requirements such as CBC operation. Only the DES-CBC algorithm is mandatory to promote interoperability. Optional ESP ciphers include 3DES, CAST, and Blowfish.

Internet Key Exchange (IKE)

- **Often called ISAKMP/Oakley**
- **Exchanges keys securely over network**



Internet Key Exchange

A concept central to IPsec is the Security Association (SA). Security Associations define the parameters used between encrypting devices and the processing done on packets passed between them. The purpose of IKE is to establish SA's and the associated shared security parameters and authenticated keys. The IKE protocol operates inside a framework defined by ISAKMP – the Internet Security Association and Key Management Protocol - and is a hybrid of the Oakley and SKEME protocols. ISAKMP defines packet formats, retransmission timeouts, and basic requirements for message construction. Oakley and SKEME define the steps taken by peers to establish a shared authenticated key. IKE is a general-purpose security exchange protocol, which conforms to the ISAKMP language. RFC-2407 defines a "Domain of Interpretation" or DOI for IKE messages used in establishing IPsec SA's. IKE itself uses SA's between parties to securely exchange information that sets up subsequent IPsec SA's. A rich set of implementation options makes IKE extremely flexible and extensible, but subsequently complex. The IKE protocol is performed by the same devices intending to use IPsec and establishes roles of "initiator" and "responder."

A "Security Association"

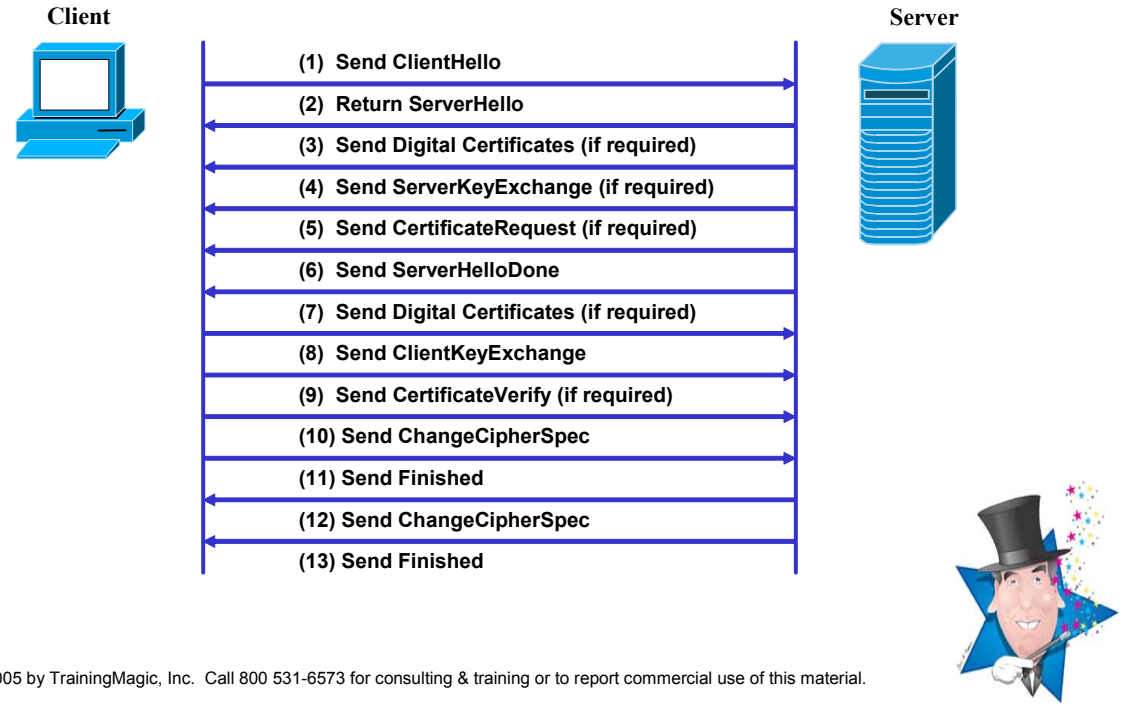
- **Each Security Association contains:**
  - **Sequence number counter**
  - **Sequence counter overflow**
  - **Anti-replay window**
  - **AH information**
  - **ESP information**
  - **Lifetime of this security association**
  - **IPSec protocol mode**
  - **Path MTU**

A "Security Association"

Security Associations (SA) are the contract between communicating parties that determine the IPsec protocols to be used (AH/ESP/both), transforms, keys, key lifetimes, and more. IPsec devices store this information in a SA database (SADB). SA's are a simplex, or one-way function. For parties to send and receive data securely, SA's must be established for each direction of transfer. SA's are also protocol specific. If two parties are using both AH and ESP, there will be an SA for each protocol in each direction. Each SA is identified in the SADB by a 32-bit "Security Parameter Index". This number appears in the header of each packet transmitted and is used to determine what processing must be applied to received packets. Packets which arrive at a receiver which does not have that SPI in their SADB are discarded.

While IPsec allows numerous options to be selected, a specific implementation will define acceptable parameters in a Security Policy Database (SPD). The SPD and its reflected *policy* define what protocols to use in what modes and the specific transforms to be used.

Sample IPsec Operation



Sample IPsec Operation

The diagram above depicts the basic steps to a generic IPsec exchange. Depending on the options invoked, certain steps may be omitted or actually require several packets to complete.

Tunneling Considerations

- Routing
  - Metrics, Loops
- Maximum Transfer Unit
  - Adjust for tunneling overhead
- Firewalls
  - Tunneling protocol pass thru…
- Performance…
  - Significant processing & transmission overhead

Tunneling Considerations

One major concern when tunneling for intranet applications involves the passage of routing information. When a simple, hub-and-spoke topology is implemented, with only one path (the tunnel) available between the branch and HQ, static routes provide all the info necessary. However, when multiple tunnels are available, or when split tunneling is allowed at the branch, great caution must be given to routing updates, default route distribution, and metric assignment. Because the tunnel appears by default as a single-hop path to a destination, it should be selected before any route (other than a direct-connected route.) But when multiple routes and tunnels exist, which should take precedence? This can be biased by assigning varying metrics to the tunnels and allowing the routing protocol to decide. Just be careful when assigning metrics or loops could occur.

A second concern arises when using intermediate connectivity, which limits the maximum packet or frame size, commonly called the Maximum Transfer Unit or MTU. In these cases, it may be necessary to account for the additional overhead of the tunneling protocols themselves. If the tunneling overhead added to the user data exceeds the MTU of some intermediate network, transmissions risk being discarded. Because IP itself includes a means of fragmenting packets, many routers can fragment the IP-encapsulated transmission to allow transfer. But this adds overhead, and risks subsequent discarding from transiting firewalls that prohibit fragments. Reducing the MTU in the end stations' configurations is one solution for this.

Another firewall-related concern emerges when VPN terminations are placed behind another firewall. This practice requires the firewall to recognize tunneled traffic in both directions, and forward to the appropriate device.

VPN Tech Comparison

	FR	ATM	MPLS	IP-Tunneling
Authenticity	Assumed	Assumed	Assumed	Signatures & Hashes
Confidentiality	Assumed	Assumed	Assumed	Encryption
Throughput	CIR/EIR	SCR/PCR	Contract, Varies	Private-Good Public-???
Availability	Contract 99.8%+	Contract 99.8%+	Contract, Varies	Private-Good Public-???
Processing Overhead	Minimal (LAPF)	Moderate (AAL, ATM)	Minimal (Labels)	High (when encrypting)

VPN Technology Comparison

The chart above lists the attributes of Frame Relay (FR), Asynchronous Transfer Mode (ATM), MultiProtocol Label Switching (MPLS), and IP-Tunneling (generically) with regard to various network concerns. Again the constrained optimization faced by most network operators involves getting the "most for the least." That is to say, for a given set of performance expectations, which solution costs the least?

Summary

- VPN: an alternative to Private Lines
- FR, ATM, MPLS: alternatives to IP Tunneling
- Variety of tunneling protocols & applications
- Tunneling protocols offer:
  Confidentiality, Authenticity, Anti-replay, more…
- Denial-of-Service: remains a concern