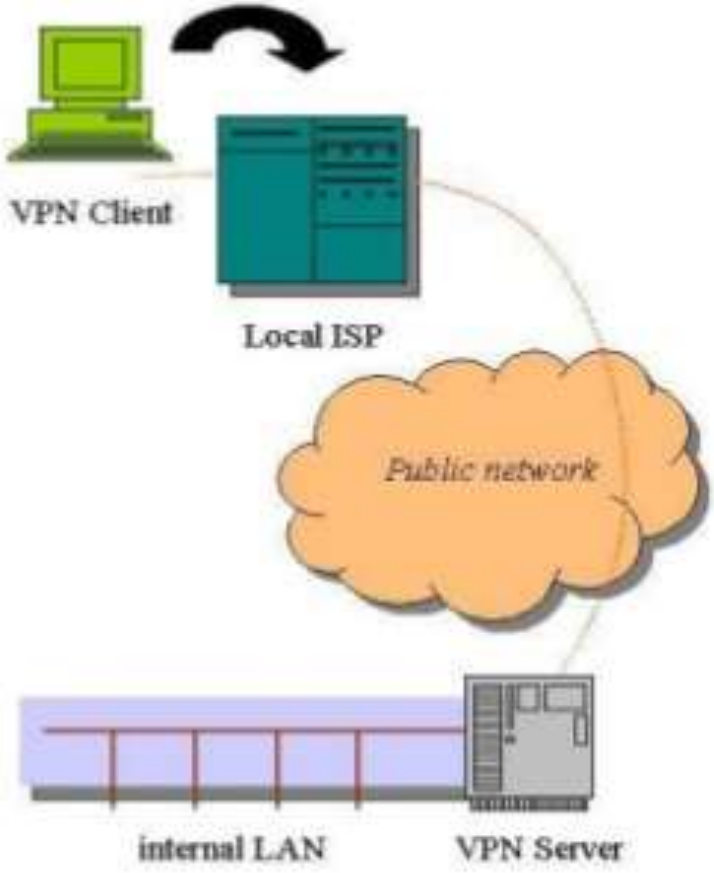
What is VPN

- Virtual Private Network is a type of private network that uses public telecommunication, such as the Internet, instead of leased lines to communicate.
- Became popular as more employees worked in remote locations.
- Terminologies to understand how VPNs work.



Introduction

Virtual. Virtual means not real or in a different state of being. In a VPN, private communication between two or more devices is achieved through a public network the Internet. Therefore, the communication is virtually but not physically there.

Private. Private means to keep something a secret from the general public. Although those two devices are communicating with each other in a public environment, there is no third party who can interrupt this communication or receive any data that is exchanged between them.

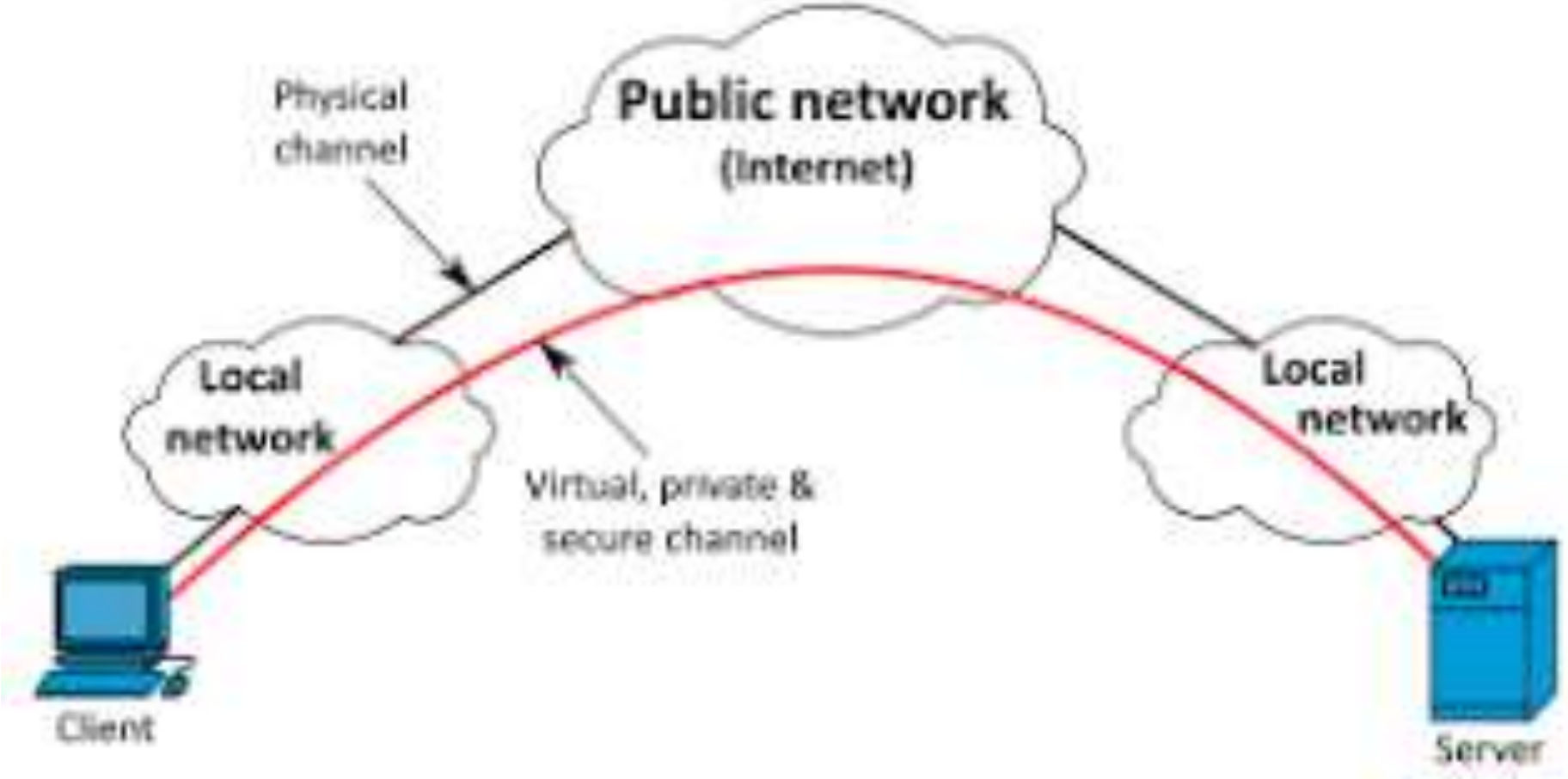
Network. A network consists of two or more devices that can freely and electronically communicate with each other via cables and wire. A VPN is a network. It can transmit information over long distances effectively and efficiently.

contin….

1. A VPN is a combination of software and hardware that allows mobile employees, telecommuters, business partners, and remote sites to use a public or "unsecured" medium such as the Internet to establish a secure, private connection with a host network.

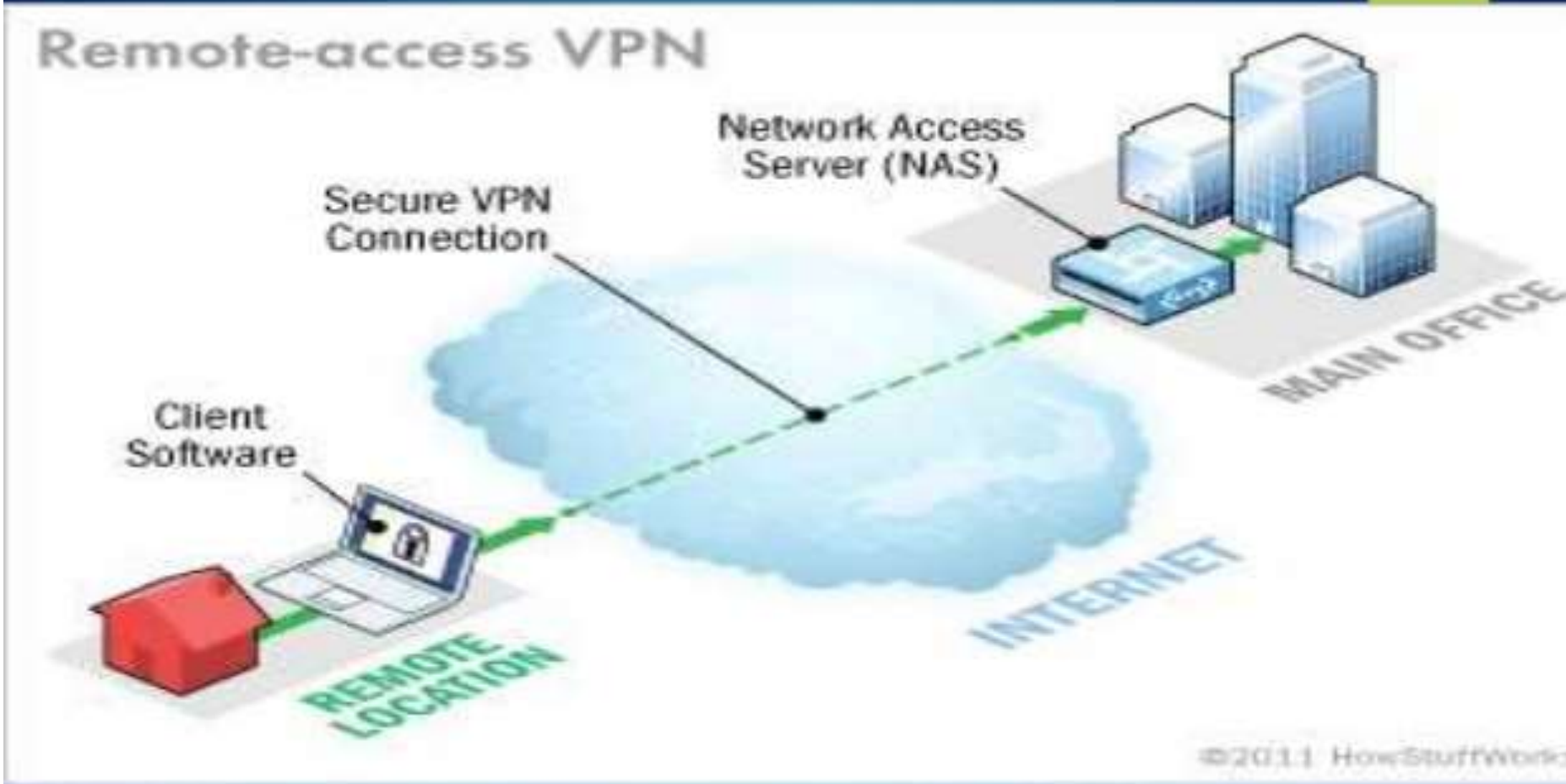
2. It uses "virtual" connections routed through the internet from the business's private network to the remote site.

3. VPN extends a private network and the resources contained in the network across public networks like the Internet.


Physical
channel
Public network
(Internet)
Local
network
Local
network
Virtual, private &
secure channel
Client
Server

What is a VPN ?

Virtual Private Network, is defined as a network that uses public network paths but maintains the security and protection of private networks. For example, Delta Company has two locations, one in Noida, New Delhi (A) and Pune, Mumbai (B). In order for both locations to communicate efficiently, Delta Company has the choice to set up private lines between the two locations. Although private lines would restrict public access and extend the use of their bandwidth, it will cost Delta Company a great deal of money since they would have to purchase the communication lines per mile. The more viable option is to implement a VPN. Delta Company can hook their communication lines with a local ISP in both cities. The ISP would act as a middleman, connecting the two locations. This would create an affordable small area network for Delta Company.



A remote-access VPN connection allows an individual user to connect to a private business network from a remote location using a laptop or desktop computer connected to the internet.

Types of VPNs

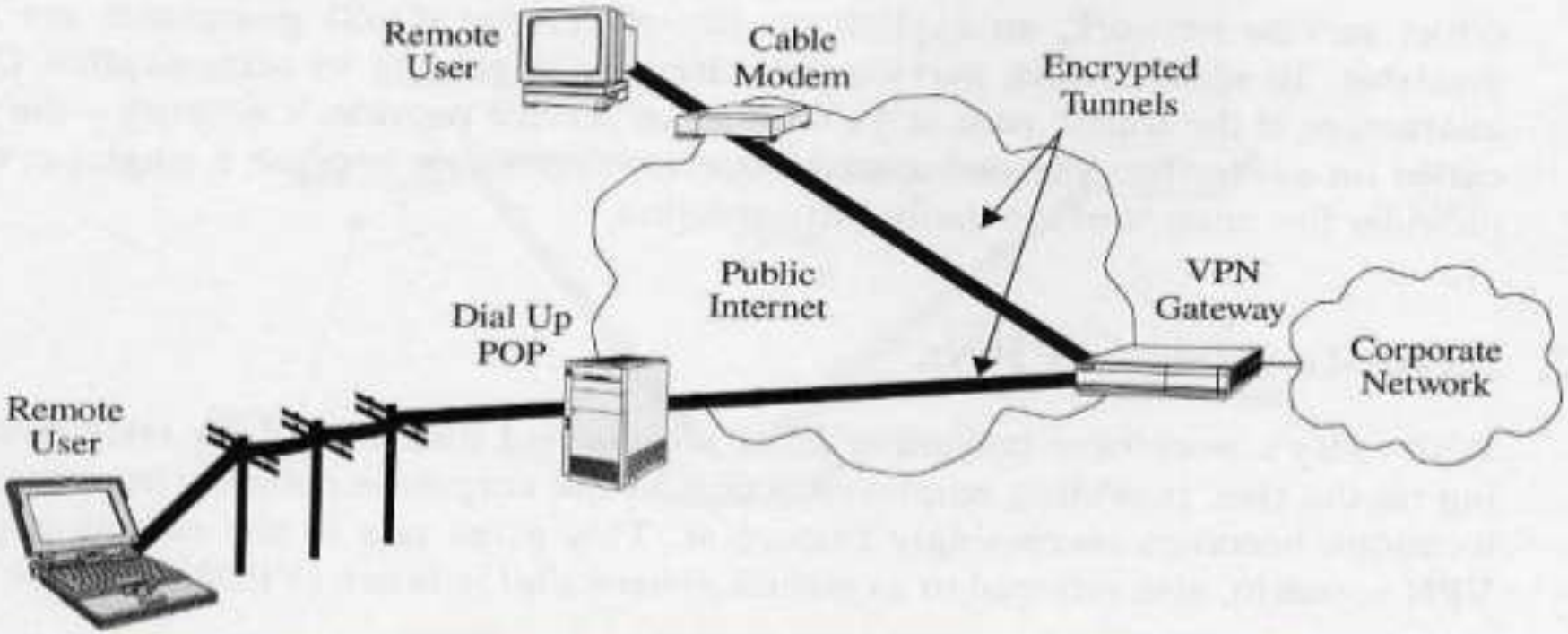
- Remote access VPN
- Intranet VPN
- Extranet VPN

Remote-Access VPN

- A remote access VPN is for home or travelling users who need to access their central LAN from a remote location.
- They dial their ISP and connect over the internet to the LAN.
- This is made possible by installing a client software program on the remote user's laptop or PC that deals with the encryption and decryption of the VPN traffic between itself and the VPN gateway on the central LAN.

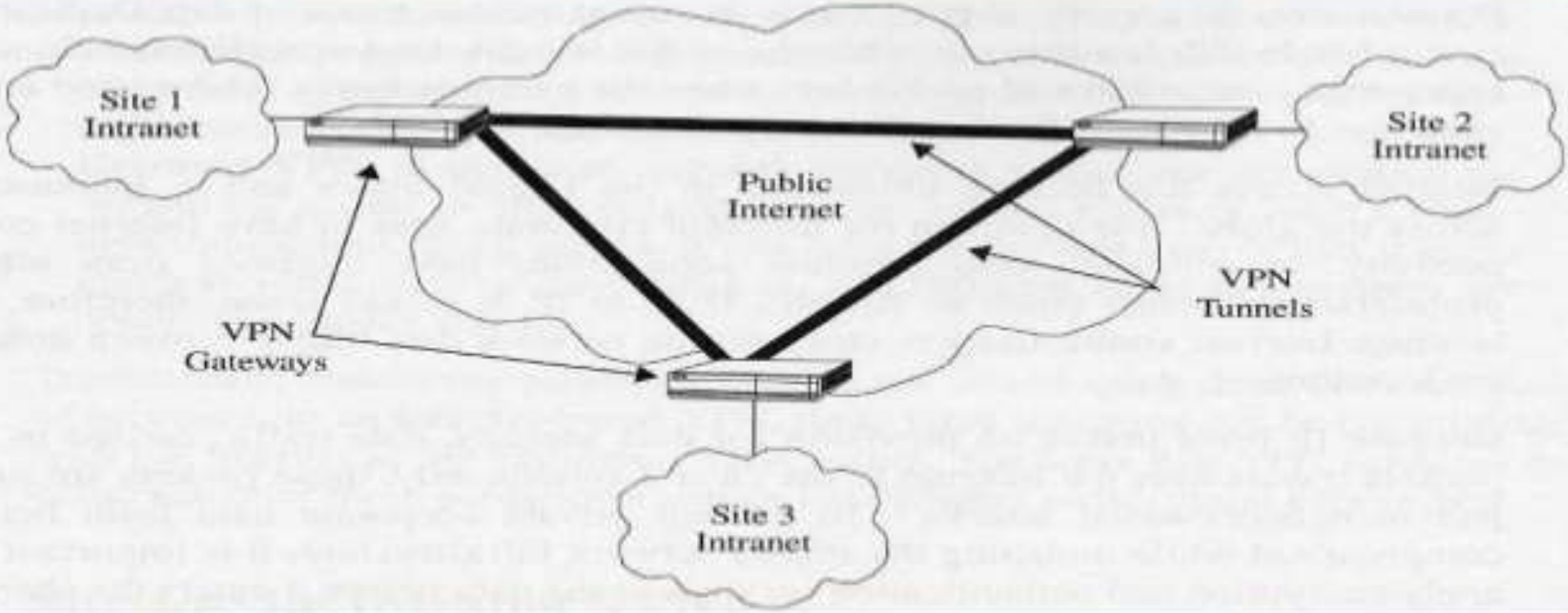
Types of VPNs

Remote access VPNs – Enable remote connectivity using any Internet access technology. The remote user launches the VPN client to create a VPN tunnel to the gateway.



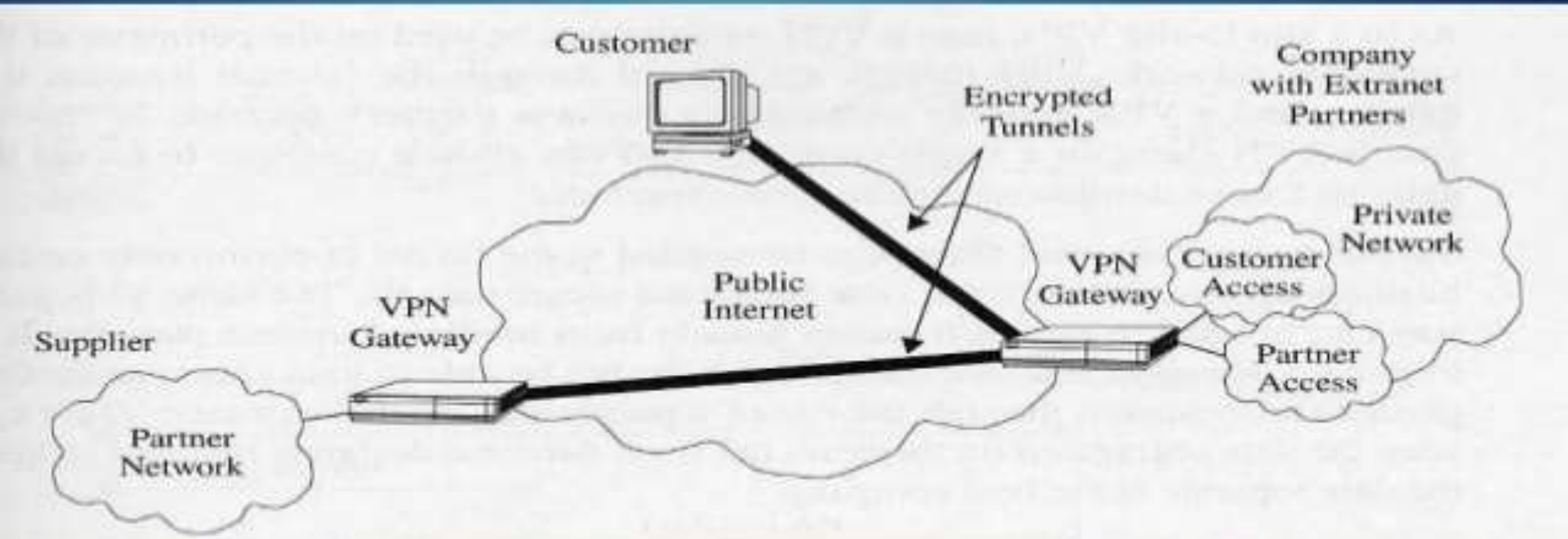
Types of VPNs

Intranet VPNs - If a company has one or more remote locations that they wish to join in a single private network, they can create an intranet VPN to connect LAN to LAN.



Types of VPNs

Extranet VPNs – When a company has a close relationship with another company (for example, a partner, supplier or customer), they can build an extranet VPN that connects LAN to LAN, and that allows all of the various companies to work in a shared environment.



Types of VPN protocols

- PPTP--Point-to-Point Tunneling Protocol
- L2TP -- Layer 2 Tunneling Protocol
- IPsec-- Internet Protocol Security
- SSL -- Secure Socket Layer

1.Point-to-Point Tunneling Protocol(PPTP)

PPTP (**P**oint-to-**P**oint **T**unneling **P**rotocol) it's the most widely supported VPN method among Windows users and it was created by Microsoft in association with other technology companies. The disadvantage of PPTP is that it *does not provide encryption and it relies on the PPP* (Point-to-Point Protocol) protocol to implement security measures. But compared to other methods, PPTP is faster and it is also available for Linux and Mac users.

2.Layer 2 Tunneling Protocol(L2TP)

L2TP (**L**ayer **2** **T**unneling **P**rotocol) it's another tunneling protocol that supports VPNs. Like PPTP, L2TP does not provide encryption and it relies on PPP protocol to do this. The difference between PPTP and L2TP is that the second one provides not only d*ata confidentiality but also data integrity*. L2TP was developed by Microsoft and Cisco as a combination between PPTP and L2F(Layer 2 Forwarding).

3.Internet Protocol Security(IPsec)

IPsec protocol can be used for *encryption in correlation with L2TP* tunneling protocol. It is used as a "protocol suite for securing Internet Protocol (IP) communications by authenticating and encrypting each IP packet of a data stream". IPSec requires expensive, *time consuming client installations* and this can be considered an important disadvantage.

4.Secure Socket Layer(SSL)

SSL (**S**ecure **S**ocket **L**ayer) is a VPN accessible via https over web browser. The advantage of this SSL VPN is that it doesn't need any software installed because *it uses the web browser as the client application*. Through SSL VPNs the user's access can be restrict to specific applications instead of allowing access to the whole network.

VPNs - Advantages

- Eliminate the need for expensive private or leased lines
- Reduce the long-distance telephone charges
- Reduced equipment costs (modem banks, CSU/DSUs)
- Reduced technical support
- Scalability – easy adding of new locations to the VPN
- Security
- Simple Management
- Lower Cost

VPN Advantages

- Multiple telephone lines and banks of modems at the central site are not required.
- A reduction in the overall telecommunication infrastructure – as the ISP provides the bulk of the network.
- Reduced cost of management, maintenance of equipment and technical support.
- Simplifies network topology by eliminating modem pools and a private network infrastructure.
- VPN functionality is already present in some IT equipment.

VPNs - Disadvantages

- Require an in-depth understanding of public network security issues and taking proper precautions in VPN deployment.
- The availability and performance of a corporate VPN (over the Internet) depends on uncontrollable external factors.
- Shortage of standardization. The products from different vendors may not work well together.
- VPNs need to accommodate complicated protocols other than IP.

VPN Disadvantage

- If the ISP or Internet connection is down, so is the VPN.
- The central site must have a permanent internet connection so that remote clients and other sites can connect at anytime.
- VPNs may provide each user with less bandwidth than a dedicated line solution.
- Existing firewalls, proxies, routers and hubs may not support VPN transmissions.

VPN Security: Firewall

A well-designed VPN uses several methods for keeping your connection and data secure:

- **Firewalls**
- **Encryption**
- **IPSec**
- **AAA Server**

- You can set firewalls to restrict the number of open ports, what type of packets are passed through and which protocols are allowed through.

VPN Devices

- Hardware
- Firewall
- Software

VPN Features

- **Security** – tunneling support between sites with at least 128bit encryption of the data.
- **Scalability** – extra users and bandwidth can be added easily to adapt to new requirements.
- **Services** – quality of service features, including bandwidth, management and traffic shaping, are important to avoid congestion.
- **Management** – reports on user activity, management of user policies and monitoring of the VPN as a whole.

What is network-layer confidentiality ?

Between two network entities:

- sending entity encrypts datagram payload, payload could be:
  - TCP or UDP segment, ICMP message, OSPF message ….
- All data sent from one entity to other would be hidden:
  - web pages, e-mail, P2P file transfers, TCP SYN packets …
- "blanket coverage"

Virtual Private Networks (VPNs)

motivation:

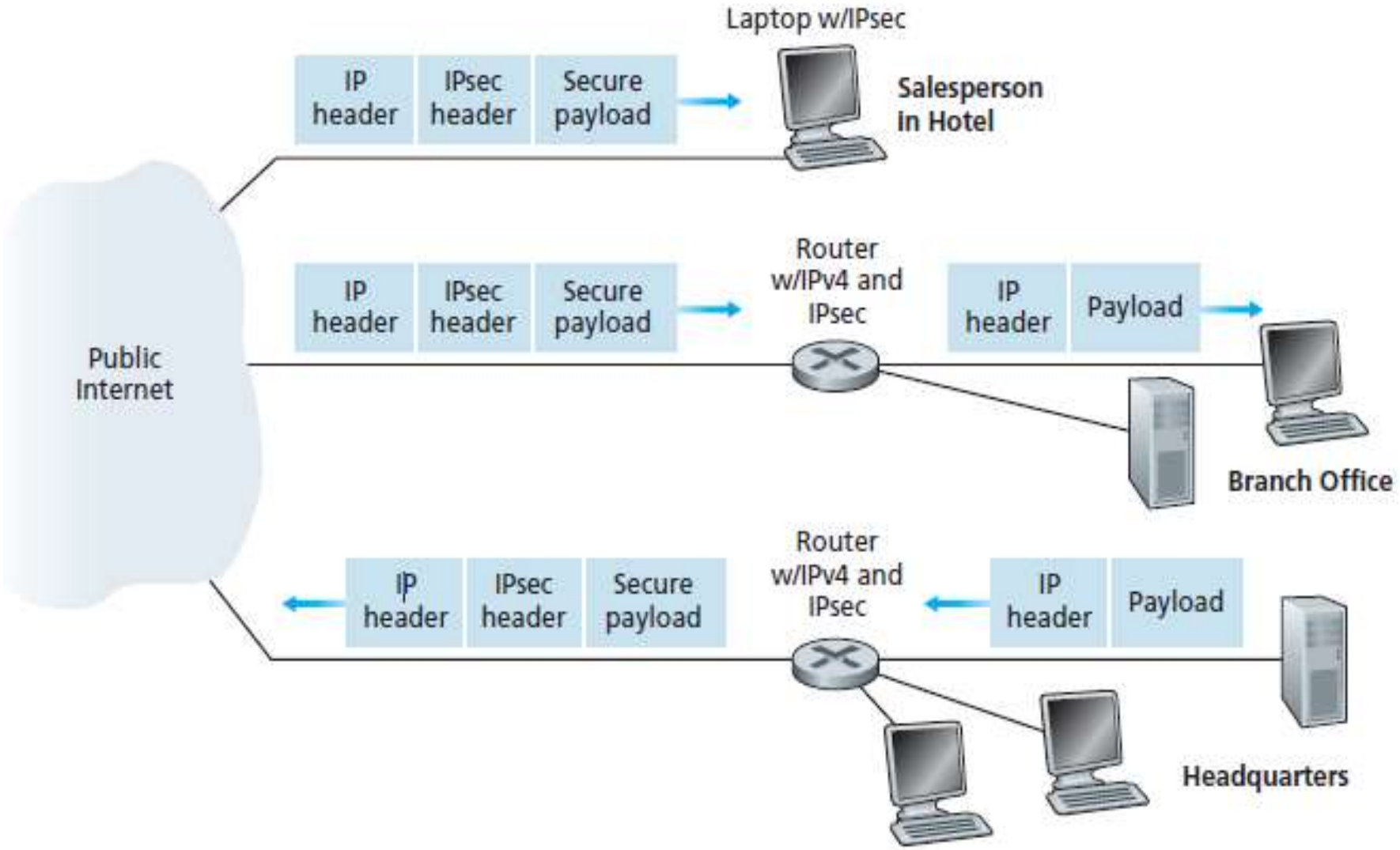
Institutions often want private networks for security

- To achieve this goal, the institution could actually deploy a stand-alone physical network—including routers, links, and a DNS infrastructure—that is completely separate from the public Internet.
- Such a disjoint network, dedicated to a particular institution, is called a **private network**.
  - costly: separate routers, links, DNS infrastructure.

•VPN: institution's inter-office traffic is sent over public Internet instead

  - encrypted before entering public Internet
  - logically separate from other traffic

Virtual Private Network



Virtual Private Network

- When a host in headquarters sends an IP datagram to a salesperson in a hotel, the gateway router in headquarters converts the IPv4 datagram into an IPsec datagram and then forwards this IPsec datagram into the Internet.

- This IPsec datagram actually has a traditional IPv4 header, so that the routers in the public Internet process the datagram as if it were an ordinary IPv4 datagram—to them, the datagram is a perfectly ordinary datagram.

Virtual Private Network

- The payload of the IPsec datagram includes an IPsec header, which is used for IPsec processing; furthermore, the payload of the IPsec datagram is encrypted.

- When the Ipsec datagram arrives at the salesperson's laptop, the OS in the laptop decrypts the payload (and provides other security services, such as verifying data integrity) and passes the unencrypted payload to the upper-layer protocol (for example, to TCP or UDP).

IP Security (IPSec)

- **IP Security (IPSec) is a collection of protocols designed by the Internet Engineering** Task Force (IETF) to provide security for a packet at the network level.

- IPSec helps create authenticated and confidential packets for the IP layer.

IPsec Protocol

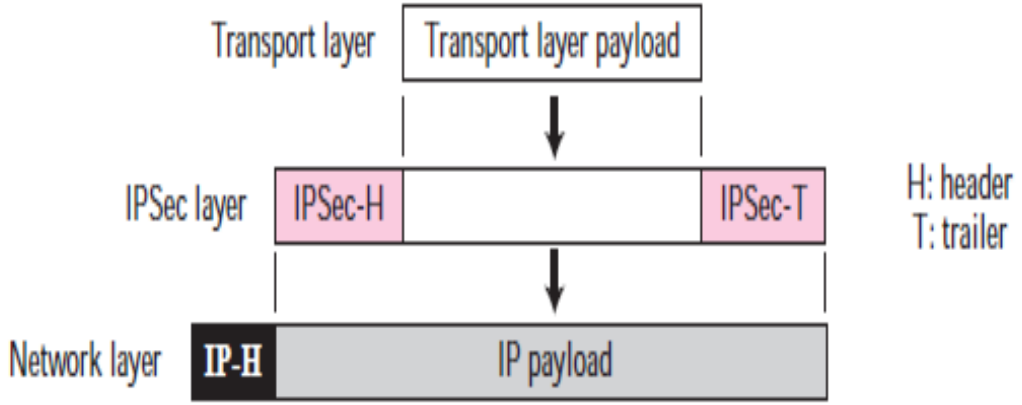
Two Modes

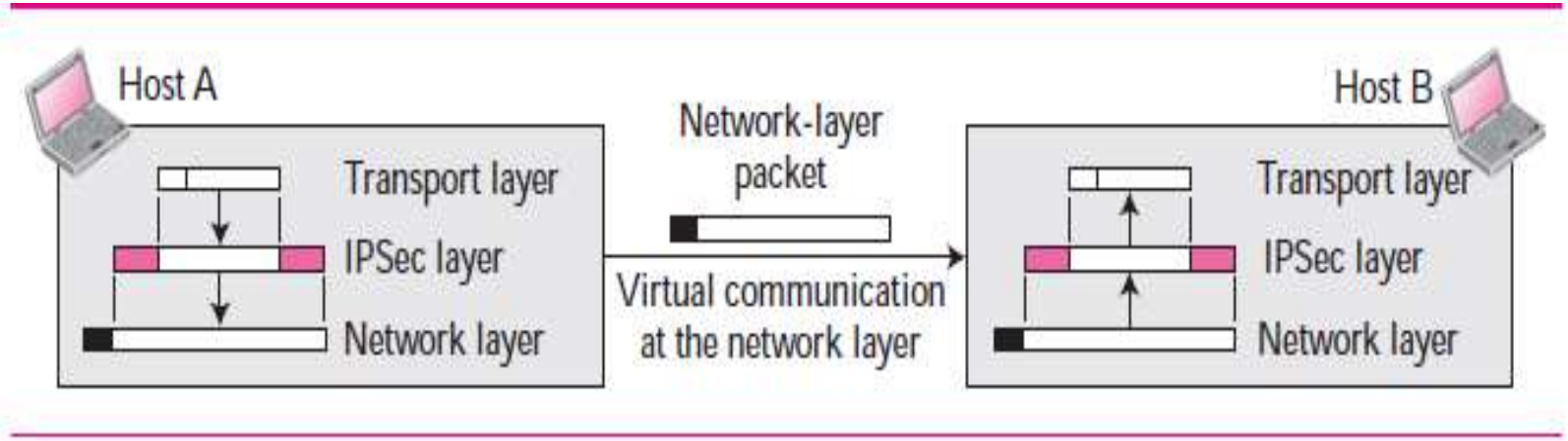
- **IPSec operates in one of two different modes: transport mode or tunnel mode.**

Transport Mode **-** In **transport mode, IPSec protects what is delivered from the transport layer to the network** layer.

- In other words, transport mode protects the payload to be encapsulated in the network layer.
- Transport mode is normally used when we need host-to-host (end-to-end) protection of data.
- The sending host uses IPSec to authenticate and/or encrypt the payload delivered from the transport layer.
- The receiving host uses IPSec to check the authentication and/or decrypt the IP packet and deliver it to the transport layer

IPSec in transport mode

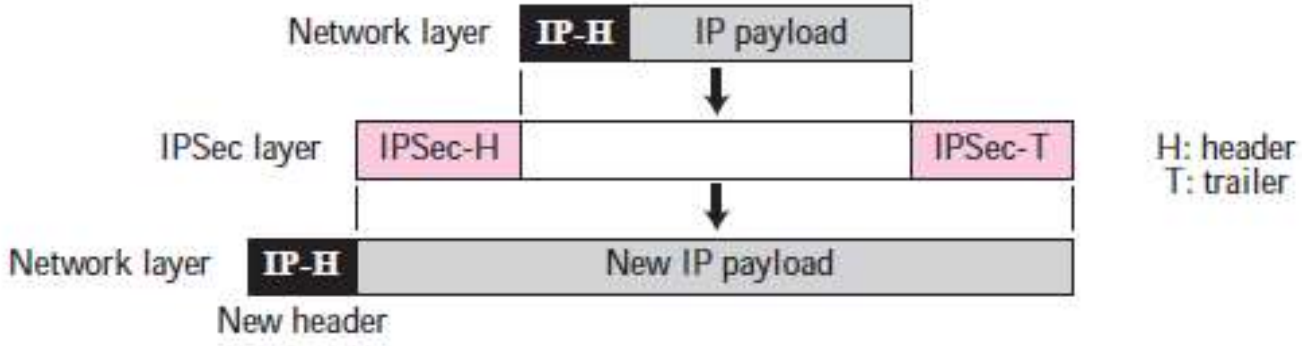




IPSec in Tunnel mode

Tunnel Mode

- In **tunnel mode, IPSec protects the entire IP packet.**
- **It takes an IP packet, including the** header, applies IPSec security methods to the entire packet, and then adds a new IP header.

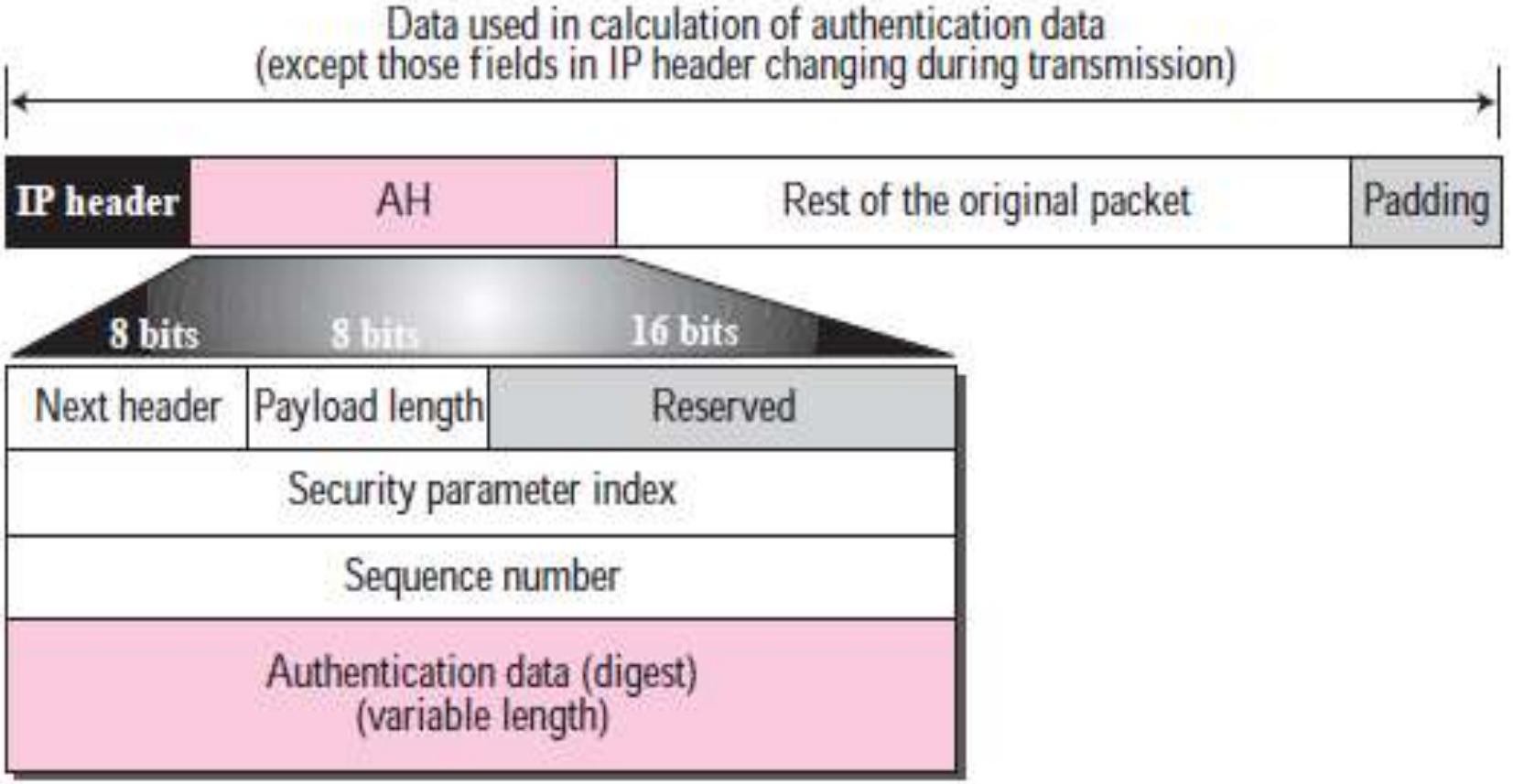


Transport mode versus tunnel mode

Two IPsec protocols

- Authentication Header (AH) protocol
  - provides source authentication & data integrity but *not* confidentiality
  - *The Authentication Header (AH) Protocol is designed to authenticate the source host*
  - *to ensure the integrity of the payload carried in the IP packet.*
  - *The protocol uses a hash function and a symmetric (secret) key to create a message digest; the digest is inserted in the authentication header*
- Encapsulation Security Protocol (ESP)
  - provides source authentication, data integrity, *and confidentiality*
  - more widely used than AH

Authentication header protocol

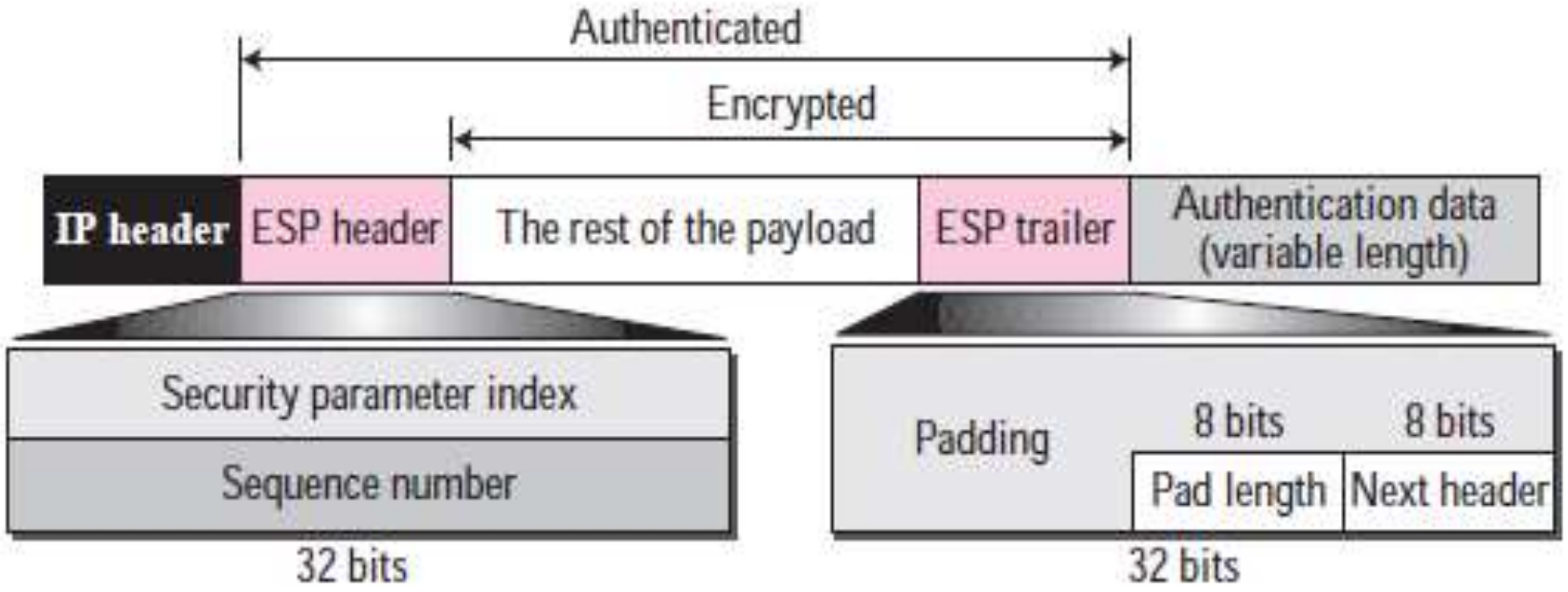


Encapsulating Security Payload (ESP)

- **Encapsulating Security Payload (ESP), that provides source authentication, integrity, and confidentiality.**

- **ESP adds a** header and trailer.
- Note that ESP's authentication data are added at the end of the packet, which makes its calculation easier.
- When an IP datagram carries an ESP header and trailer, the value of the protocol field in the IP header is 50.

ESP


Authenticated
Encrypted
IP header
ESP header
The rest of the payload
ESP trailer
Authentication data (variable length)
Security parameter index
Sequence number
32 bits
Padding
8 bits
8 bits
Pad length
Next header
32 bits

Security Association

- IPsec datagrams are sent between pairs of network entities, such as between two hosts, between two routers, or between a host and router.

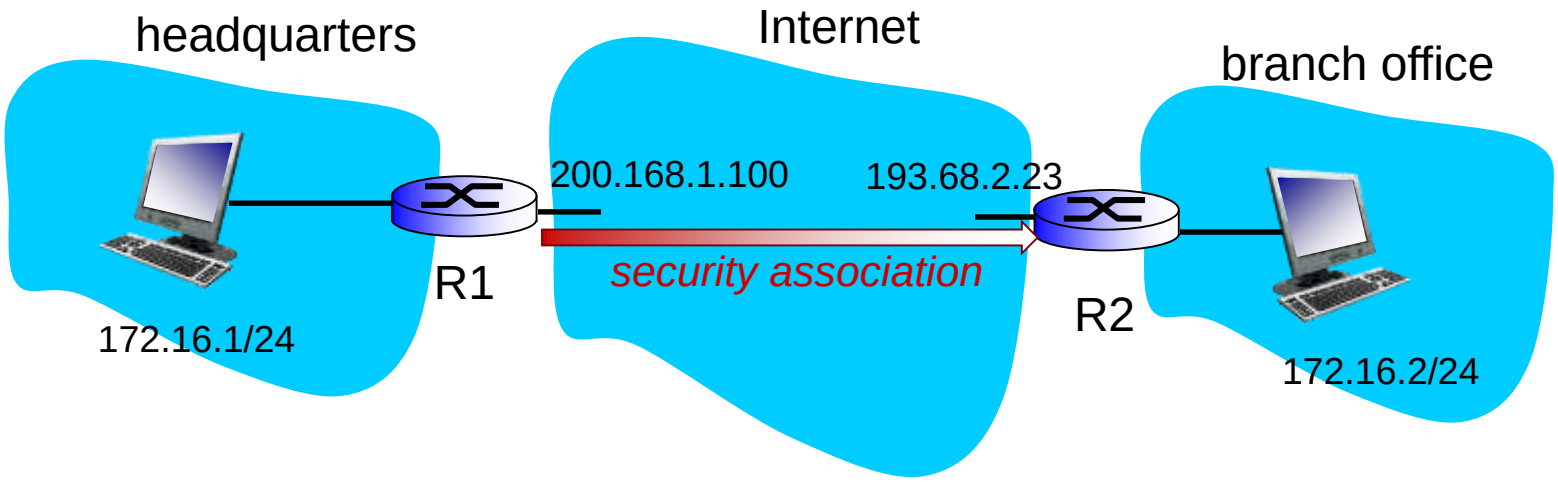
- Before sending IPsec datagrams from source entity to destination entity, the source and destination entities create a network- layer logical connection.
- This logical connection is called a **security association (SA).**
- **An SA is a simplex logical connection; that is, it is unidirectional from source to** destination.

- If both entities want to send secure datagrams to each other, then two SAs (that is, two logical connections) need to be established, one in each direction.

Security associations (SAs)

- before sending data, "security association (SA)" established from sending to receiving entity
  - SAs are simplex: for only one direction
- ending, receiving entitles maintain *state information* about SA
  - recall: TCP endpoints also maintain state info
  - IP is connectionless; IPsec is connection-oriented!

Example SA from R1 to R2



R1 stores for SA:

- 32-bit SA identifier: *Security Parameter Index (SPI)*
- origin SA interface (200.168.1.100)
- destination SA interface (193.68.2.23)
- type of encryption used (e.g., DES)
- encryption key
- type of integrity check used (e.g., HMAC with MD5)
- authentication key

Security associations (SAs)

- Whenever router R1 needs to construct an IPsec datagram for forwarding over this SA, it accesses this state information to determine how it should authenticate and encrypt the datagram.

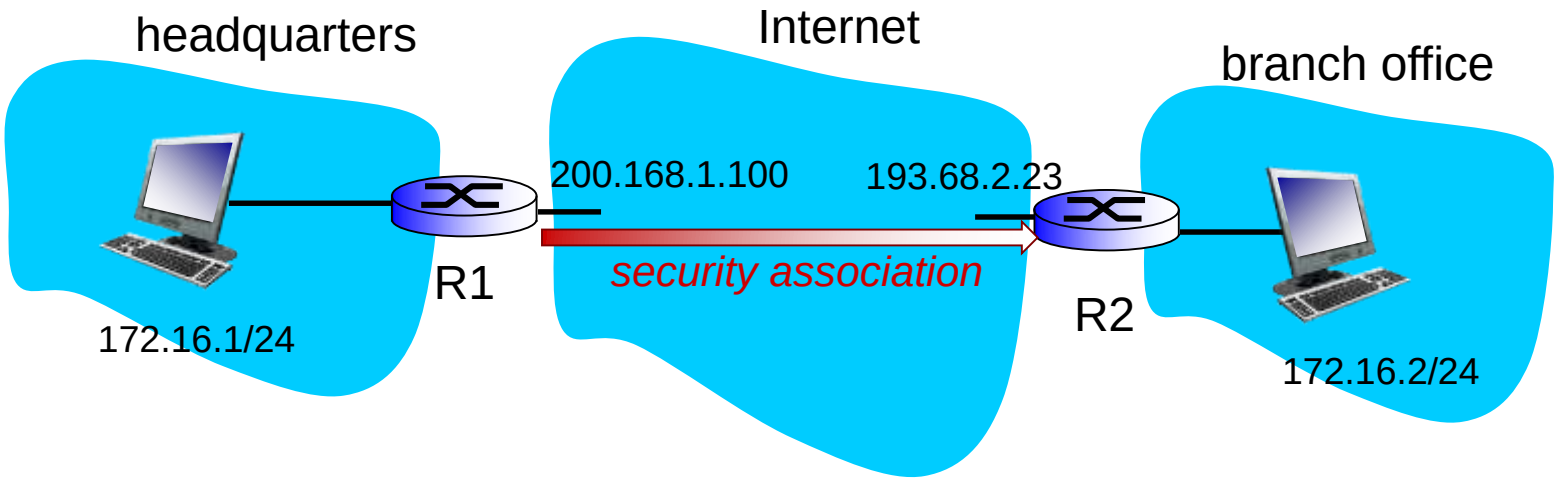
- Similarly, router R2 will maintain the same state information for this SA and will use this information to authenticate and decrypt any IPsec datagram that arrives from the SA.

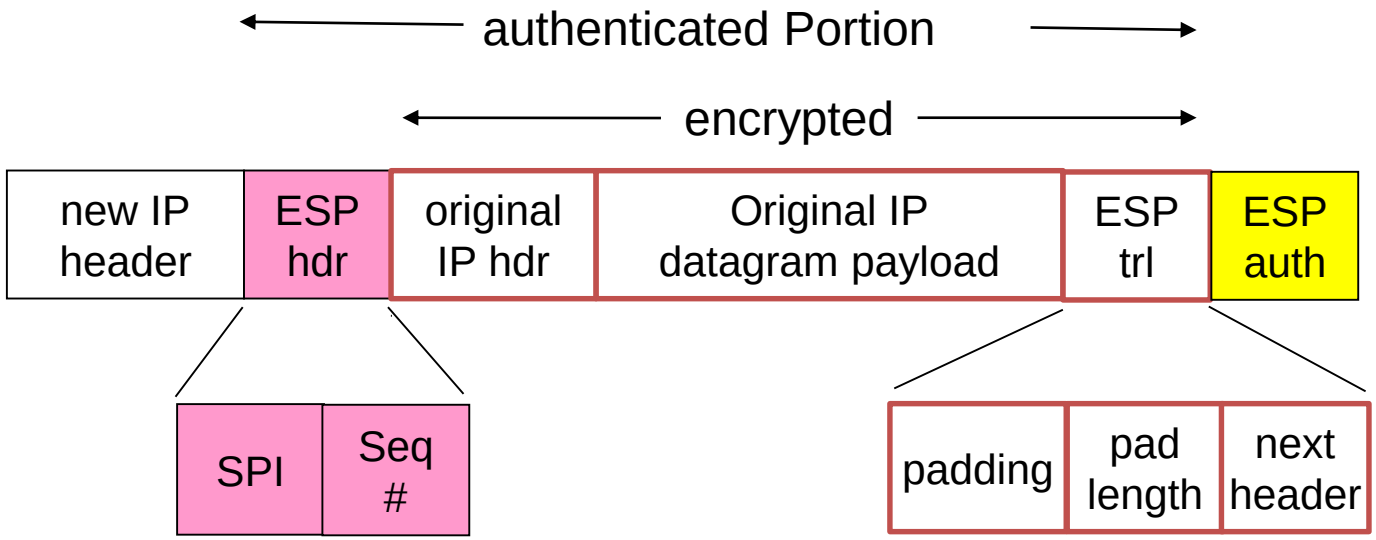
- An IPsec entity (router or host) often maintains state information for many SAs.

Security Association Database (SAD)

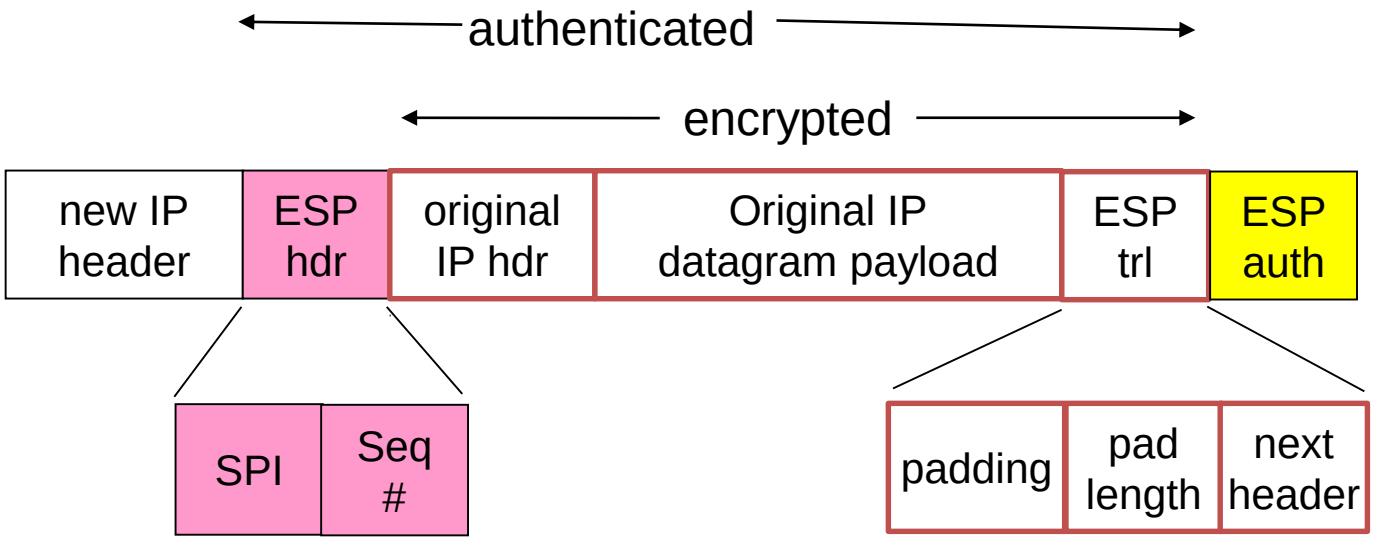
- endpoint holds SA state in *security association database (SAD)*, where it can locate them during processing.
- when sending IPsec datagram, R1 accesses SAD to determine how to process datagram.
- when IPsec datagram arrives to R2, R2 examines SPI in IPsec datagram, indexes SAD with SPI, and processes datagram accordingly.

Ipsec Datagram





Ipsec Datagram



- ESP trailer: Padding for block ciphers
- ESP header:
  - SPI 32-bit SA identifier: *Security Parameter Index (SPI)*
  - Sequence number
- MAC in ESP auth field is created with shared secret key

Ipsec Datagram

- The ESP trailer consists of three fields: padding; pad length; and next header.
- Block ciphers require the message to be encrypted to be an integer multiple of the block length.
- Padding (consisting of meaningless bytes) is used so that when added to the original datagram (along with the pad length and next header fields), the resulting “message” is an integer number of blocks.
- The pad-length field indicates to the receiving entity how much padding was inserted (and thus needs to be removed).
- The next header identifies the type (e.g., UDP) of data contained in the payload-data field.
- The payload data (typically the original IP datagram) and the ESP trailer are concatenated and then encrypted

Internet Key Exchange (IKE)

- The **Internet Key Exchange (IKE) is a protocol designed to create** Security Associations.

- when a peer needs to send an IP packet, it consults the Security Policy Database (SPD) to see if there is an SA for that type of traffic.
- If there is no SA, IKE is called to establish one.