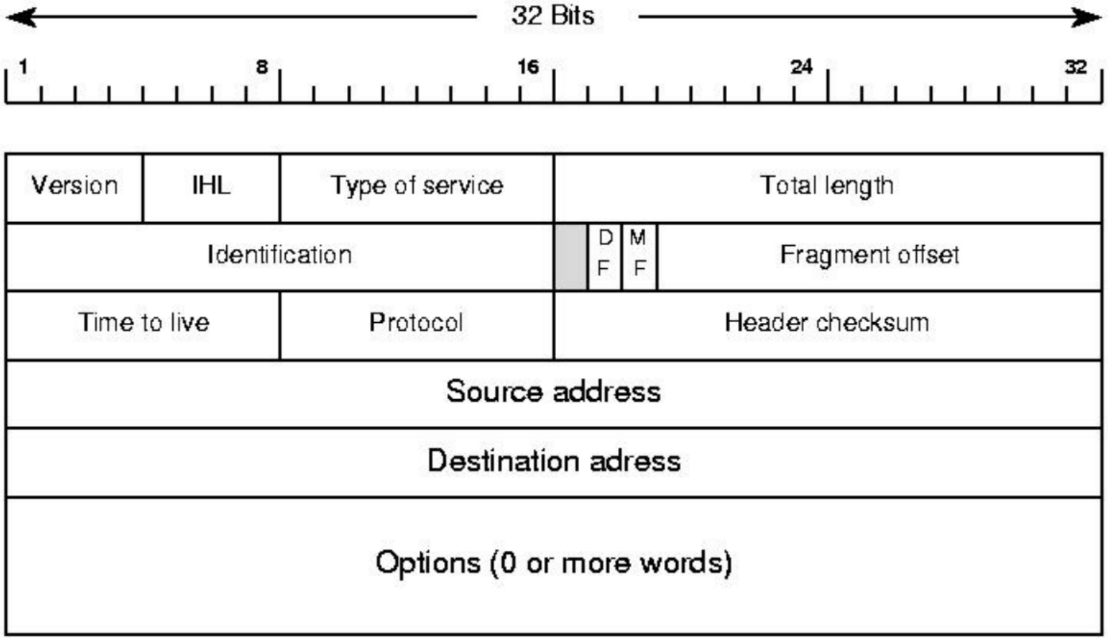
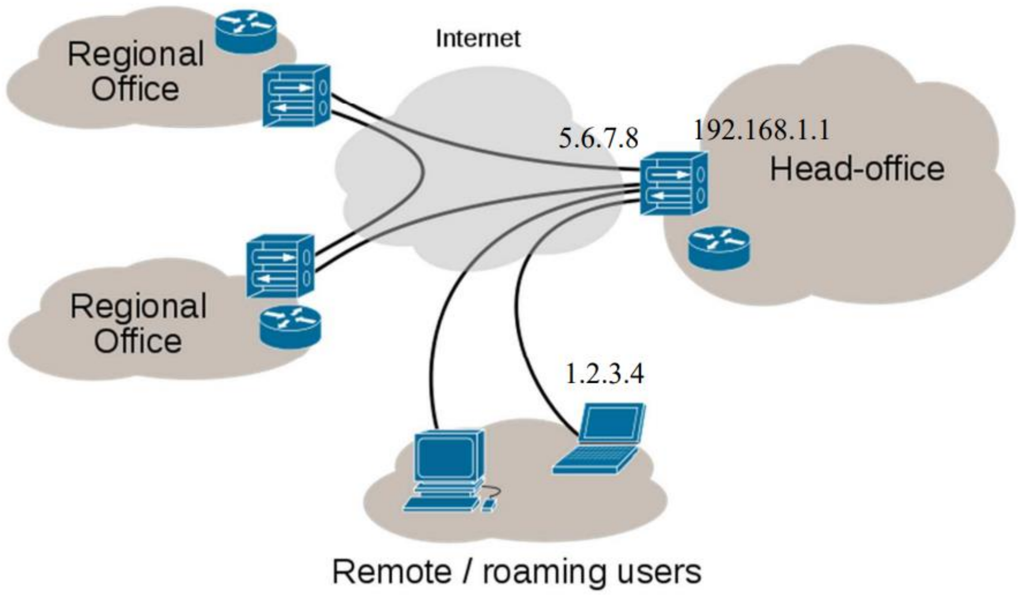

32 Bits
1
8
16
24
32
Version
IHL
Type of service
Total length
Identification
D F
M F
Fragment offset
Time to live
Protocol
Header checksum
Source address
Destination adress
Options (0 or more words)

VPN Tunnel Example

Internet VPN



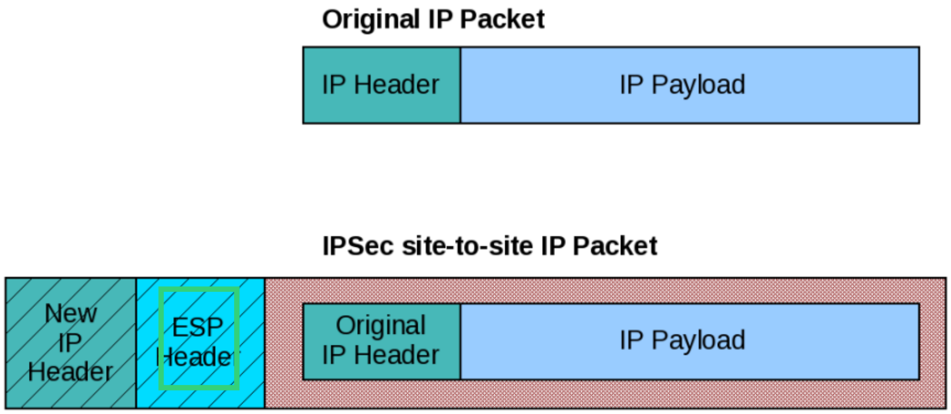
VPN Tunnel Example

- Remote host (IP address 1.2.3.4) wishes to connect to a server inside a company network
- Server has internal address 192.168.1.10 and is not reachable publicly
- Before the client can reach this server, it needs to go through a VPN server device that has public IP address 5.6.7.8 and an internal address of 192.168.1.1
- All data between the client and the server will need to be kept confidential

VPN Tunnel Example

- The VPN client connects to a VPN server via an external network interface
- The VPN server assigns an IP address to the VPN client from the VPN server's subnet
  - Client gets internal IP address 192.168.1.50,
  - Client creates a virtual network interface through which it will send encrypted packets to the other tunnel endpoint
  - This interface also gets the address 192.168.1.50
- When the VPN client wishes to communicate with company server, it prepares a packet addressed to 192.168.1.10, encrypts it and encapsulates it in an IPSec packet

VPN Tunnel Example



VPN Tunnel Example

- This packet is then sent to the VPN server at IP address 5.6.7.8 over the public Internet
- The inner packet is encrypted so that even if someone intercepts the packet over the Internet, they cannot get any information from it
  - They can see that the remote host is communicating with a VPN server, but none of the contents of the communication.
  - The inner encrypted packet has source address 192.168.1.50 and destination address 192.168.1.10.
  - The outer packet has source address 1.2.3.4 and destination address 5.6.7.8

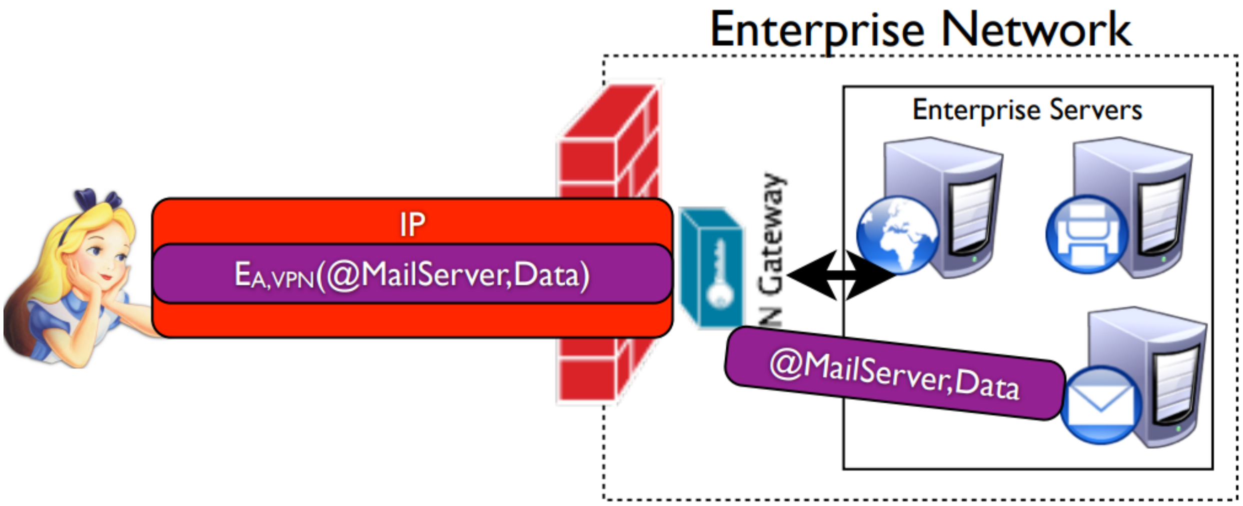
VPN Tunnel Example

- When the packet reaches the VPN server from the Internet, the VPN server:
  - Decapsulates the inner packet
  - Decrypts it
  - Finds the destination address to be 192.168.1.10
  - Forwards it to the intended server at 192.168.1.10

VPN Tunnel Example

- After some time, the VPN server receives a reply packet from 192.168.1.10, intended for 192.168.1.50
- The VPN server consults its routing table, and sees this packet is intended for a remote host that must go through VPN
- The VPN server encrypts this reply packet, encapsulates it in a VPN packet and sends it out over the Internet
- The inner encrypted packet has source address 192.168.1.10 and destination address 192.168.1.50
- The outer VPN packet has source address 5.6.7.8 and destination address 1.2.3.4
- The remote host receives the packet. The VPN client unencapsulates the inner packet, decrypts it, and passes it to the appropriate software at upper layers.

VPN Tunneling


Enterprise Network
Enterprise Servers
IP
$E_{A,VPN}$(@MailServer,Data)
N Gateway
@MailServer,Data