

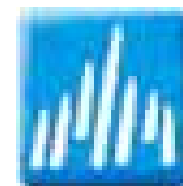
CISCO SYSTEMS



Reti Private Virtuali - VPN

Marco Misitano, CISSP

Enterprise Consulting, Security
misi@cisco.com

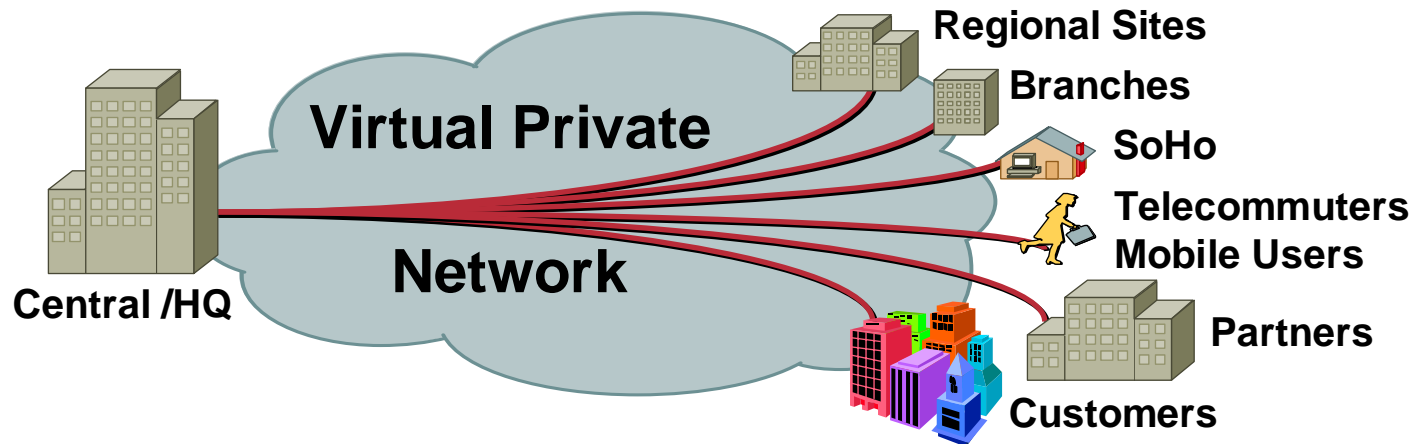


Agenda

- **Technology introduction**
- **Remote Access VPN**
- **Site to Site VPN**
- **Recap**

What is a VPN?

Connectivity deployed on a **Shared Infrastructure** with the same policies and performance as a private network



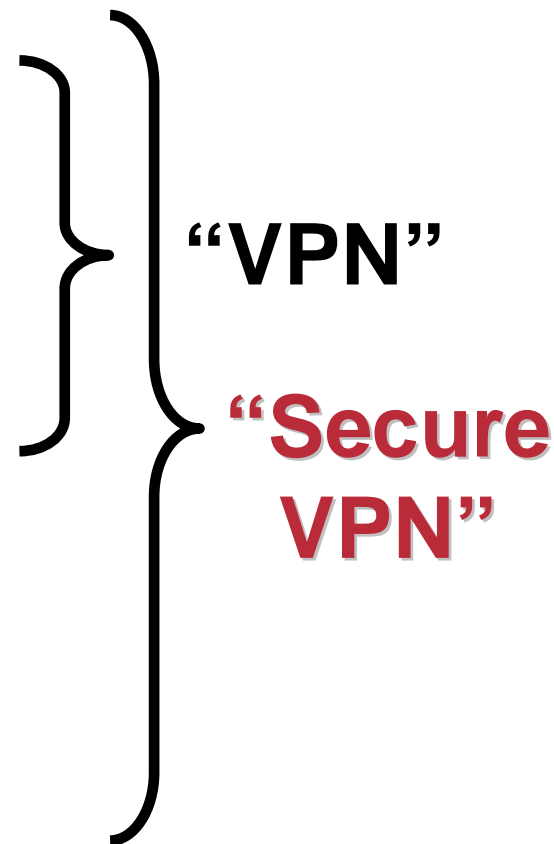
- **Address space separation**
- **Traffic separation**
- **Routing separation**

VPN Services and Technologies

	Service	Architecture	Technologies
	Access VPN	Client-Initiated NAS-Initiated	CPE and Network based IPsec, L2TP, PPTP Dial, ISDN, DSL, Cable, Wireless
site to site	Intranet VPN	IP Tunnel Virtual Circuit MPLS	CPE and Network based IPsec, GRE FR, ATM IP or IP + ATM
	Extranet VPN	IP Tunnel Virtual Circuit MPLS	CPE and Network based IPsec, GRE FR, ATM IP or IP + ATM

What is a **Secure** VPN?

- **Address space separation**
- **Traffic separation**
- **Routing separation**
- **Authentication**
- **Confidentiality**
- **Data integrity**



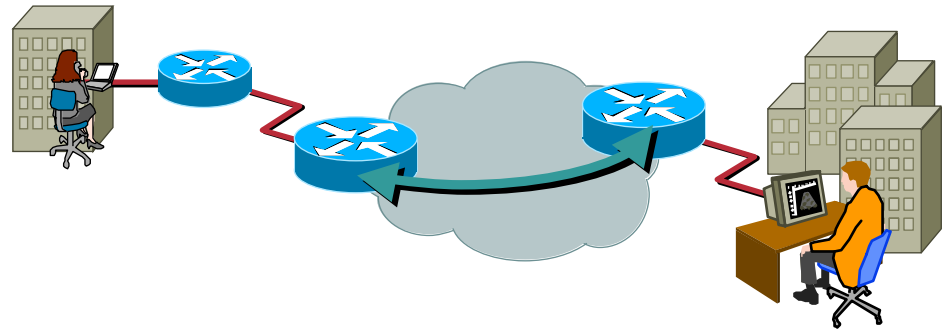
Types of VPNs

- **Site-to-site**

Between two network entities e.g. routers

Trusted networks behind each entity

Should provide performance, resilience and QoS



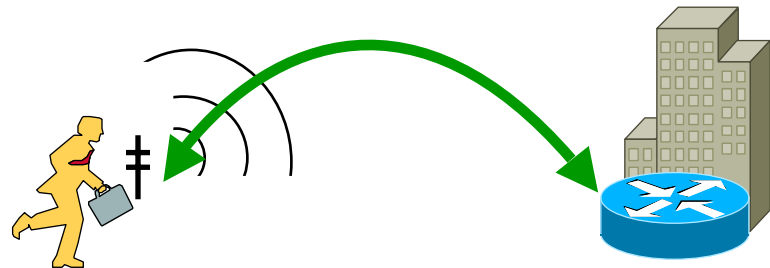
- **Remote access**

Between a host and a router

Central control of remote users

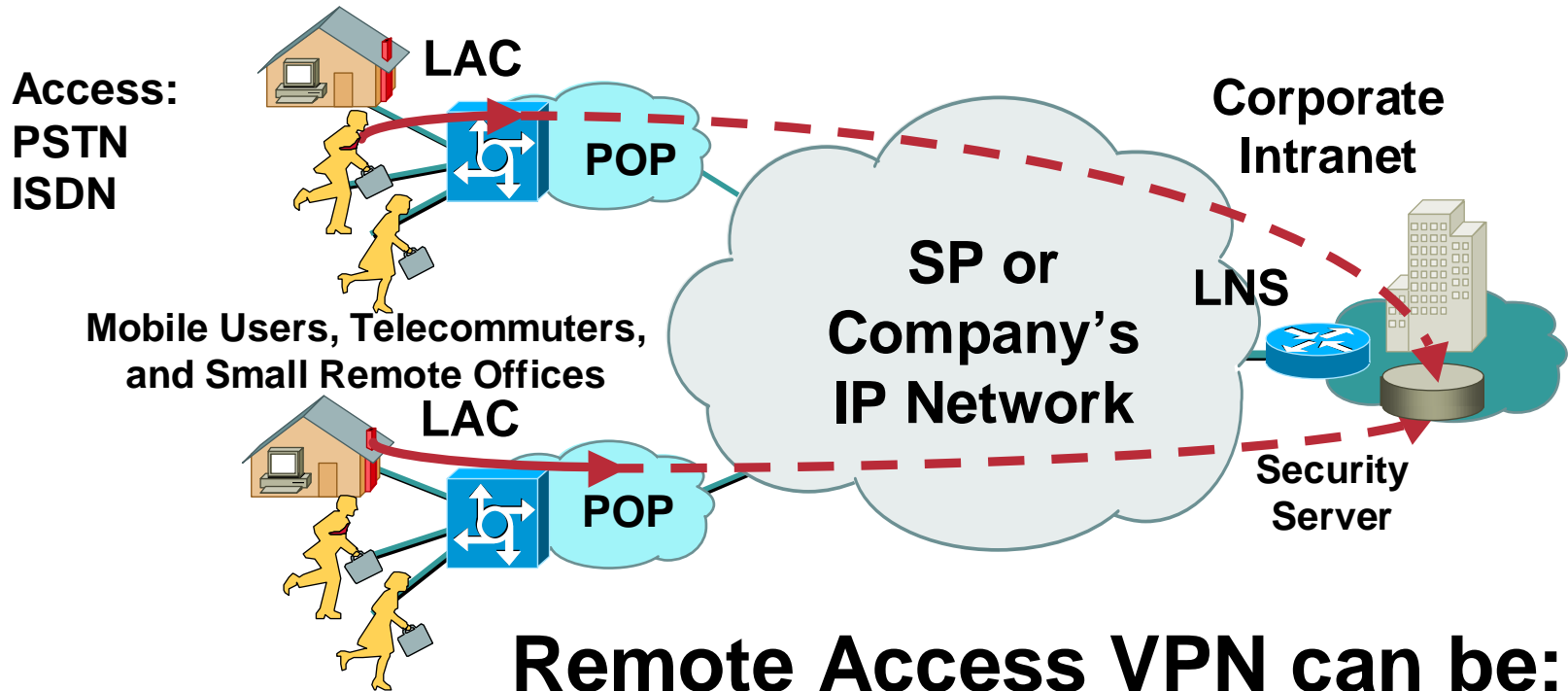
Scalable deployment

No trusted networks at remote location



Remote Access VPN

Remote Access VPNs



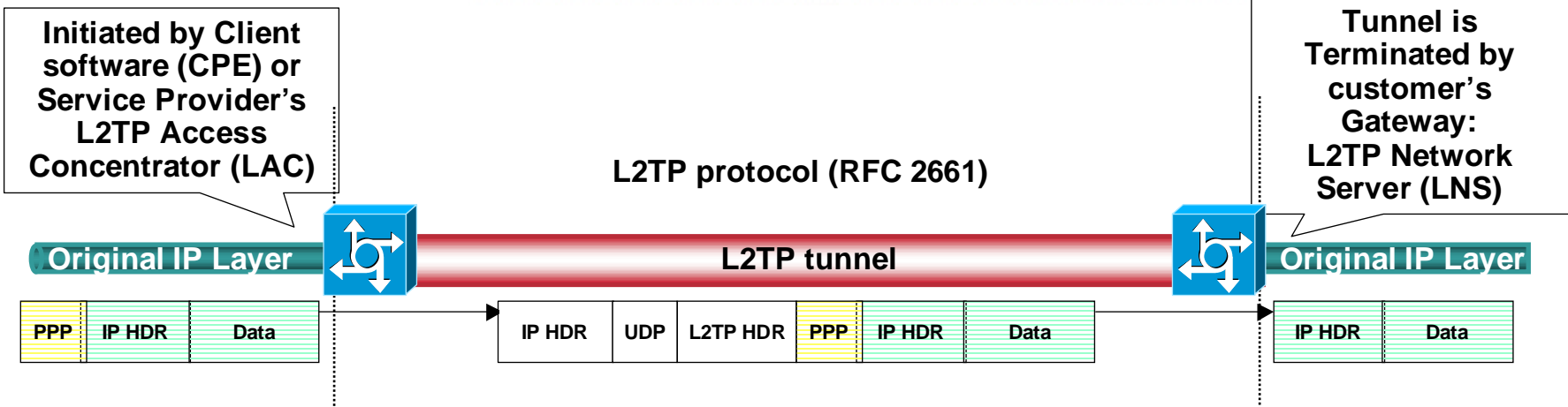
Remote Access VPN can be:

- **Client-initiated**
- **NAS-initiated**

L2TP over UDP/IP

Technology Primer

Cisco.com



- **Authorization/Addressing controlled by the Corporation or Service Provider**
- **Accounting can be performed by Service Provider/Corporation**
- **L2TP tunnel allows session multiplexing**
- **Tunnel authentication**

L2TP Remote Access VPN

Client-Initiated/NAS Initiated

Advantages	Limitations
<ul style="list-style-type: none">• L2TP is open standard (multi-vendor support)• Provisioning of VPN services without SP infrastructure changes (transparent to SP network)• Ubiquitous client software (PPTP now, L2TP with MS Win2K)• Very flexible, can span over multiple SP networks• Supports tunneling of any protocol encapsulated by PPP• Support for private addressing	<ul style="list-style-type: none">• Moderately Scalable<ul style="list-style-type: none">-No tunnel sharing so each concurrent user terminates a separate tunnel on gateway• Client software MAY need to be installed on user PC• Client Software will need to be supported (support desk costs)• No embedded security<ul style="list-style-type: none">- No Integrity- No Confidentiality• IPsec can be used to protect L2TP

Remote Access VPN: when to use?

- Need is remote access via PSTN/ISDN for: teleworkers, telecommuters, extranet users
- Scalable and manageable solution (PC client to maintain, Win2K, XP have L2TP per default)
- Standard-based interoperability
- Support of private addressing RFC1918
- Worldwide deployed solution

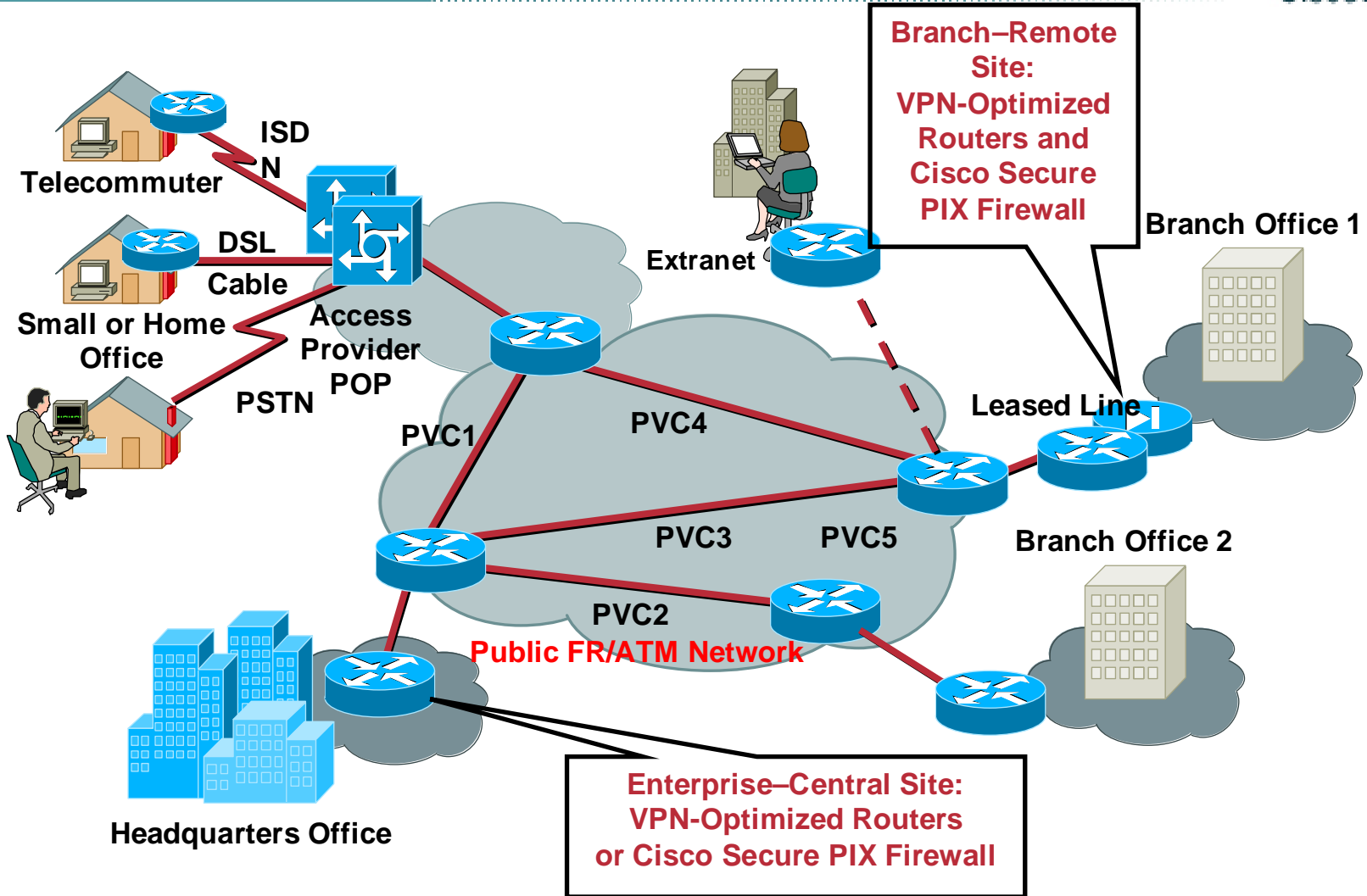
Site to Site, PVC Based VPN

Frame Relay/ATM Terminology

- **PVC: Permanent Virtual Circuit, a virtual circuit that is permanently available.**
- **ATM: Asynchronous Transfer Mode, a network technology based on transferring data in cells or packets of a fixed size.**
- **Frame Relay (FR): A packet-switching protocol for connecting devices on a Wide Area Network (WAN).**
- **LL: Leased Line, a permanent telephone connection between two points set up by a telecommunications common carrier.**

Source: www.webopedia.com

Site to Site VPN PVC Based



Site to Site VPN

PVC based

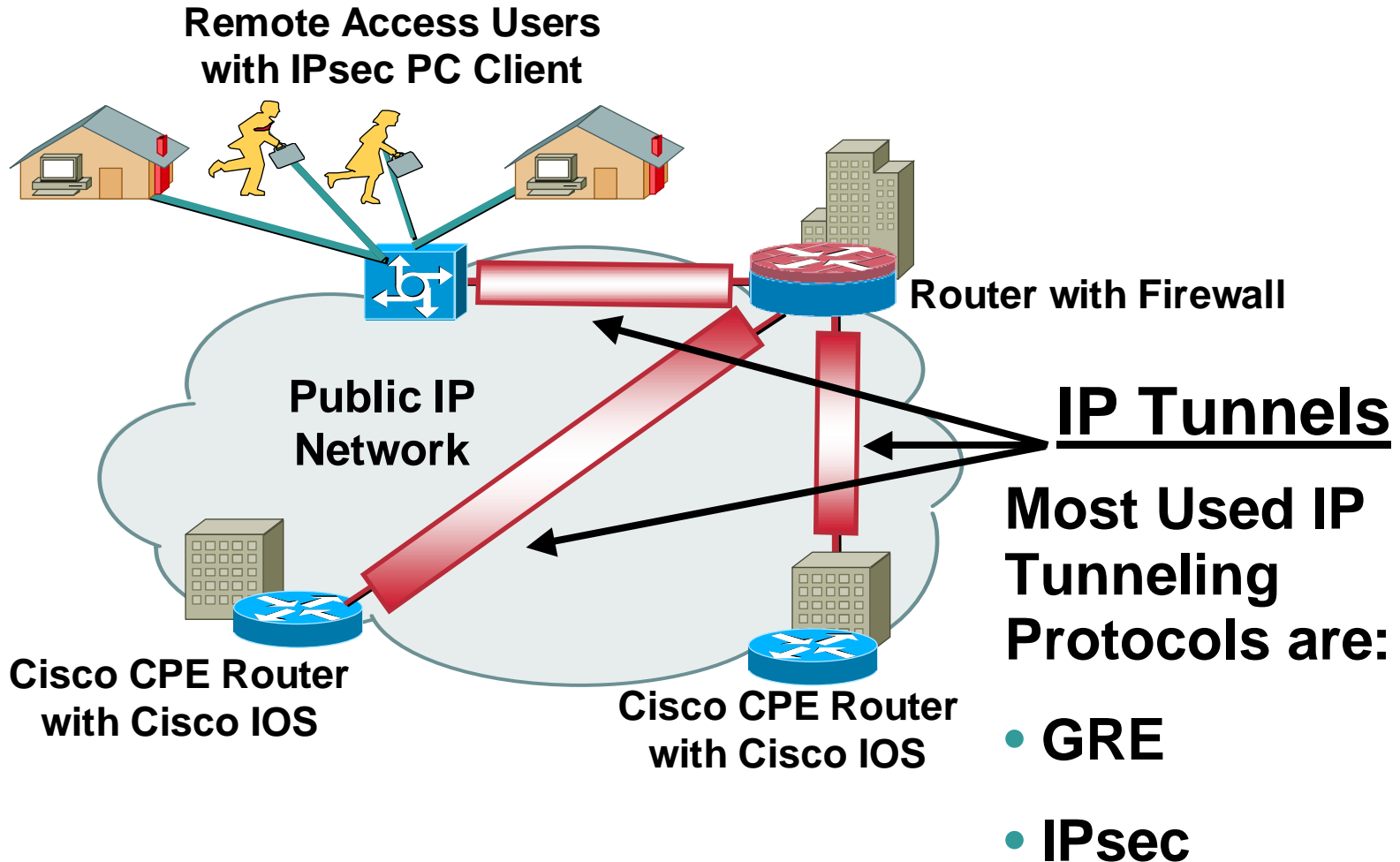
Advantages	Limitations
<ul style="list-style-type: none">• Quickly and quite inexpensively provision of VPN services from existing ATM/FR infrastructure• PVCs provide logical separation of VPN traffic and moderate to good level of security• Quick access to layer 2 QoS and SLA enforcement with established technologies such as: FR CIR, ATM SCR / MCR / PCR, etc.	<ul style="list-style-type: none">• Full point-to-point mesh required leads to N-squared scalability issues• Provisioning, maintenance and changes become time consuming for large VPNs• PVC doesn't offer security (integrity, authentication, confidentiality)• IP level QoS only available if CPE device can perform layer 4 routing and IP traffic shaping before VC• Adding new sites imply complex VPN reconfiguration• Dual Homing (redundancy) means duplicate number of connections

PVC based VPN: when to use?

- Need is to build a robust, partially meshed Intranet backbone
- Support hub-and-spoke hierarchical topology
- Support of private addressing RFC1918
- Standard based solution
- Native Layer 2 Quality of Service

Site to Site, Tunnel Based VPN

Dedicated VPNs: IP Tunnels



Site to Site, GRE Based VPN

Site to Site VPN

GRE based

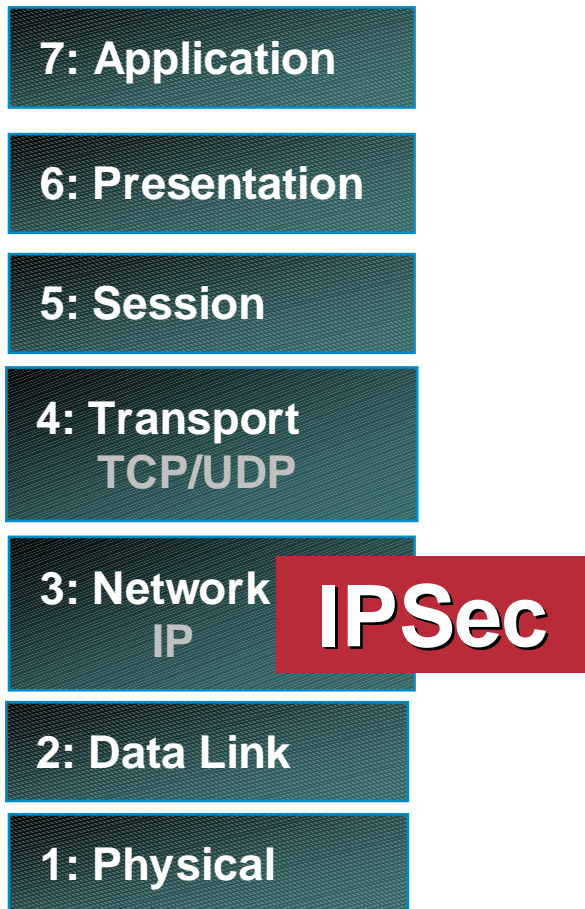
Advantages	Limitations
<ul style="list-style-type: none">• Relatively high performance tunneling• All IP QoS available• Quick deployment (available on all Cisco routers and Layer 3 switches)• Supports private addressing and traffic segregation• Supports tunneling of non-IP unicast traffic• Supports IP Multicast• Supports Intra-VPN routing	<ul style="list-style-type: none">• Overlay point-to-point mesh required leads to N-squared scalability issues• Minimal security<ul style="list-style-type: none">- No Integrity- No Authentication- No Confidentiality• QoS only possible with single, private SP networks (not over Internet)• Adding new sites imply VPN complex reconfiguration• Dual Homing (redundancy) means duplicate number of tunnels

GRE VPN: when to use?

- **Need to build an overlaid, partially meshed connectivity between few sites**
- **Support hub-and-spoke non-hierarchical topology**
- **Support of private addressing RFC1918**
- **Standard RFC-based solution**
- **Quality of Service (ToS based)**

Site to Site, IPsec Based VPN

What Is IPSec?



- **Standard for implementing Authentication, Confidentiality and Integrity on IP Networks**
- **Application Independent (Web, Mail, Voice....)**
- **Transport Independent (Leased Lines, FR, ISDN, ...)**
- **Two major components**

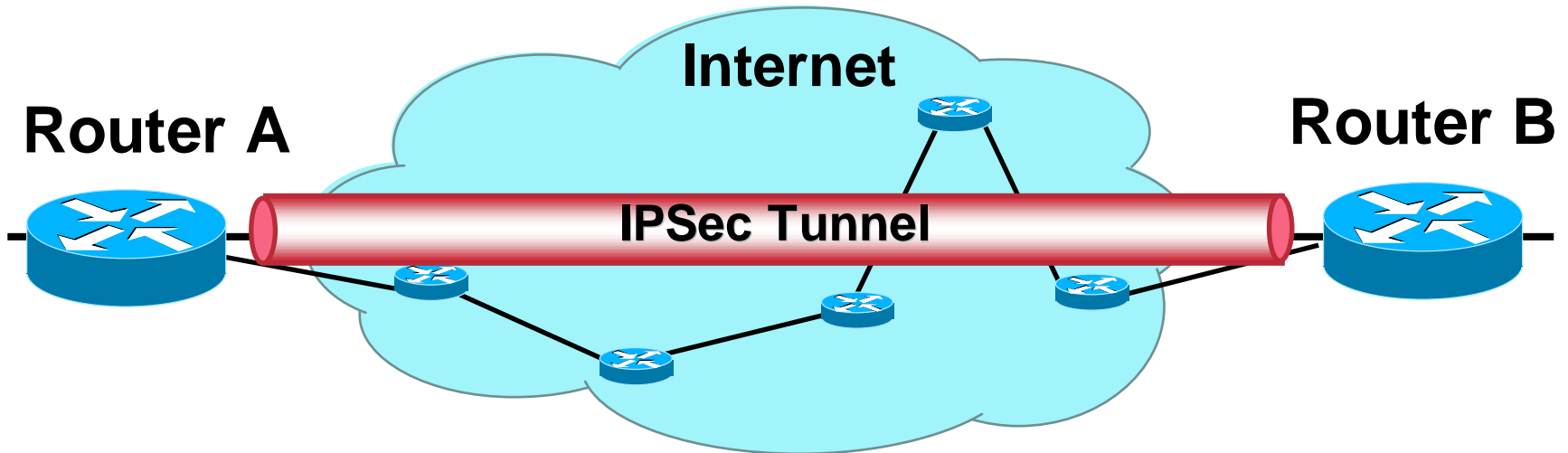
IP Security (IPSec)

Packet format to transport encrypted data

Internet Key Exchange (IKE)

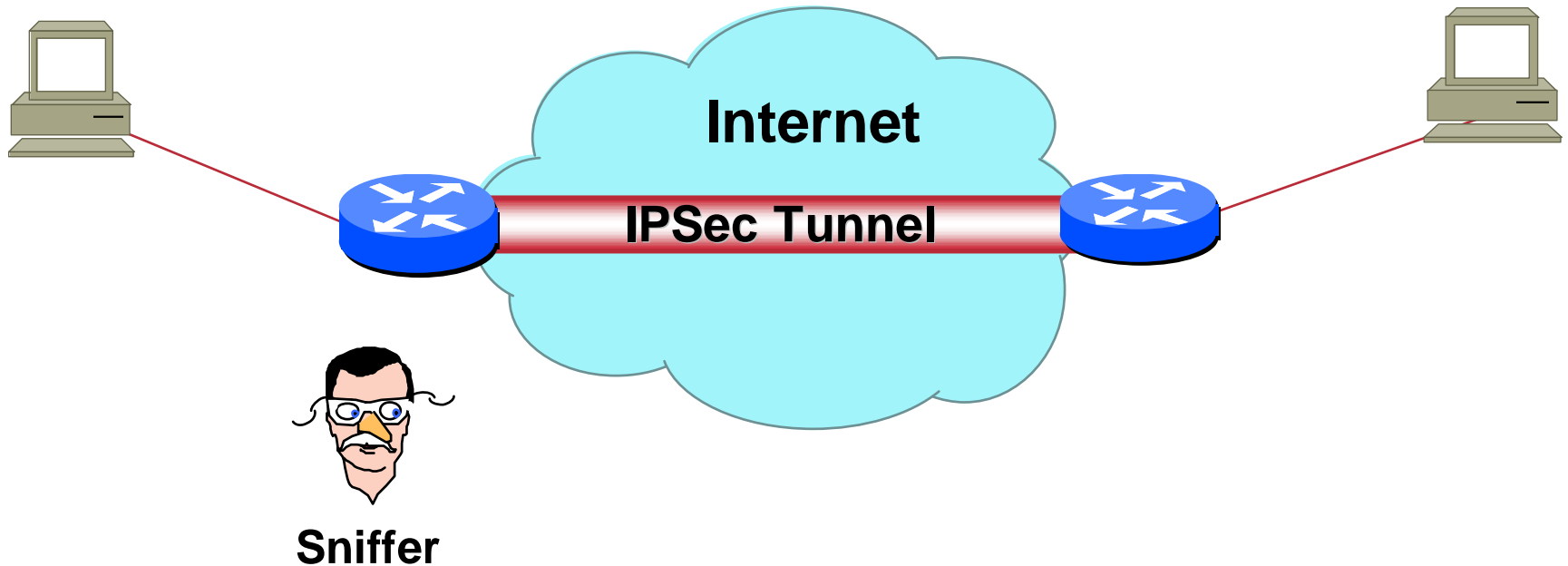
Authentication and policy negotiation between devices

Authentication



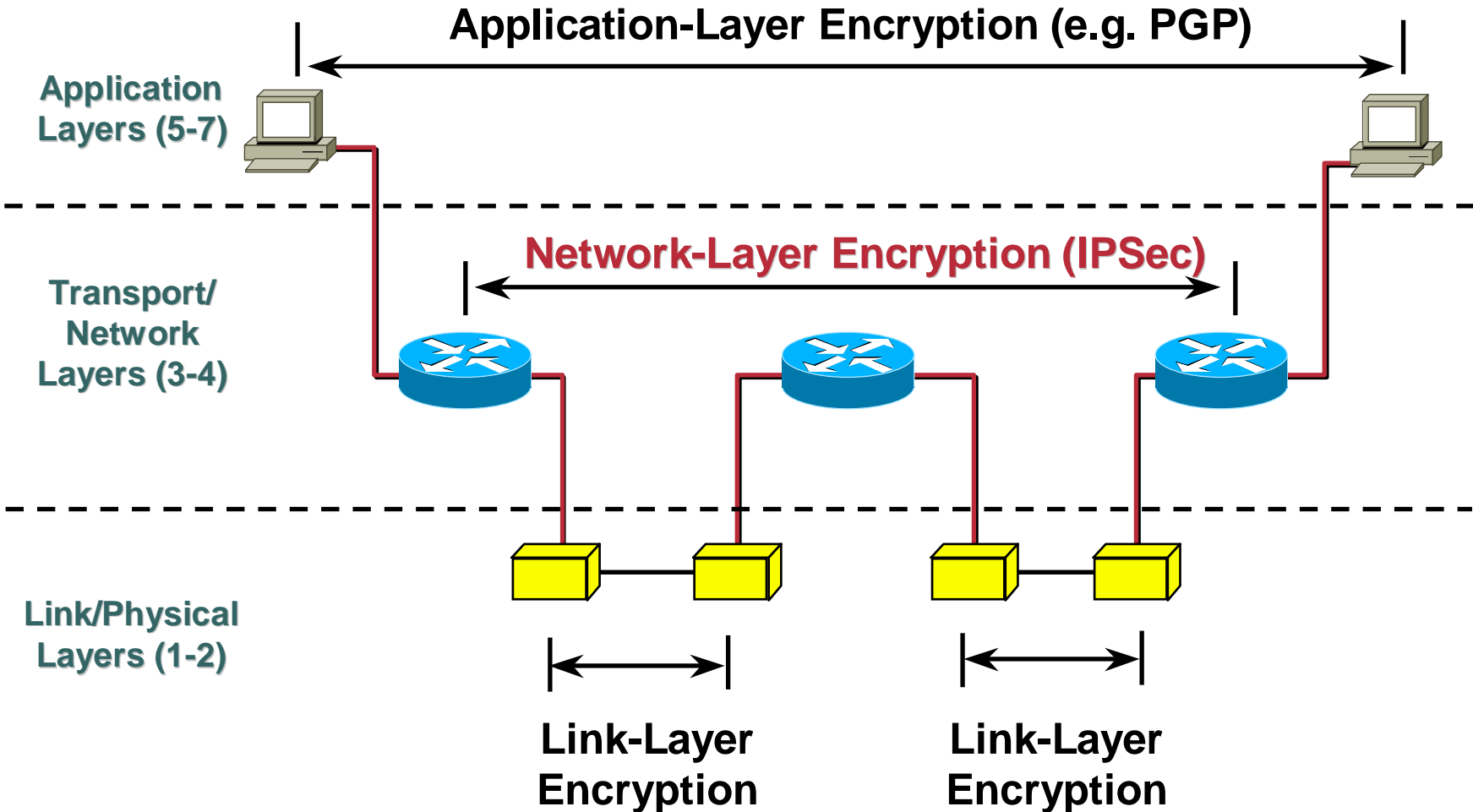
How does Router A know he is talking to Router B?

Confidentiality



Traffic across an insecure network should be encrypted for confidentiality

Encryption Alternatives



Data Integrity

- **Data received = data sent**
- **Mathematical algorithms + digital signatures (MD5, SHA-1)**



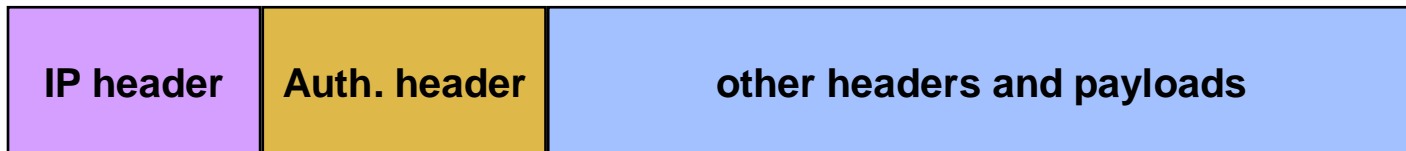
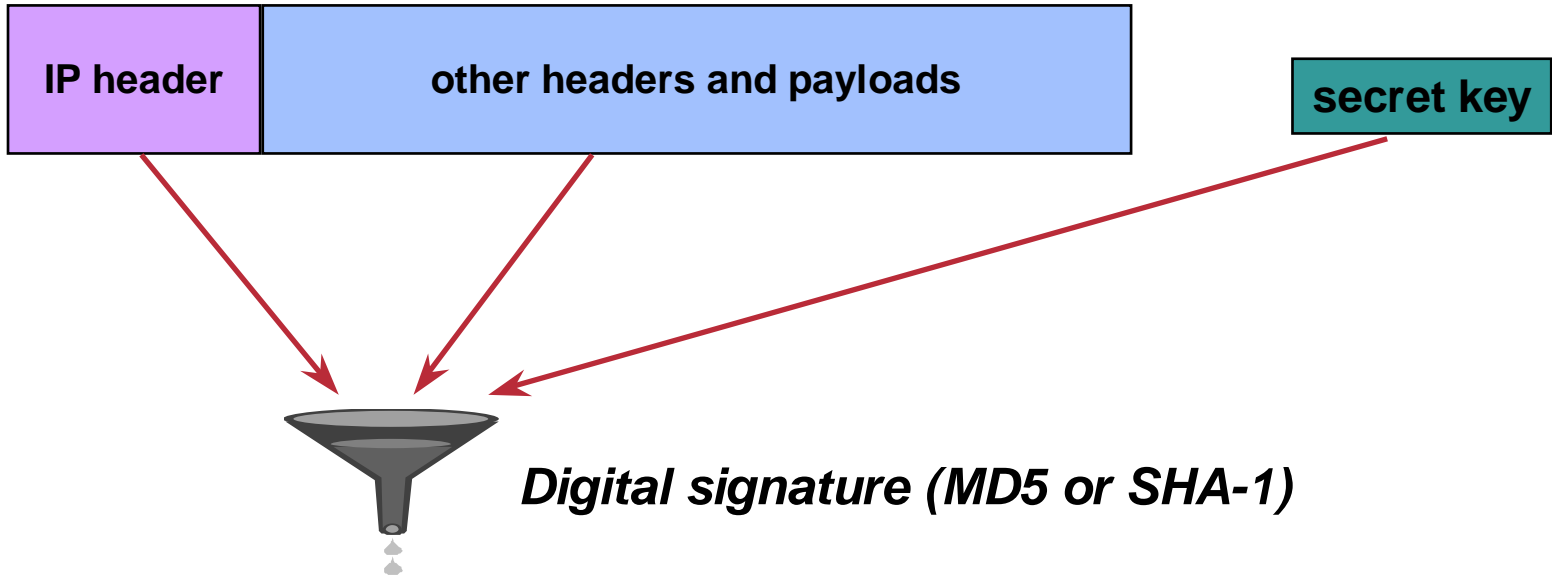
- **IPSec technologies**
 - Encapsulation types**
 - IKE
 - Encryption
 - Key management
 - Digital certificates

IPSec Authentication Header (AH)

- **RFC 2402 (Nov '98)**
- **Additional header inside the IP datagram**
- **Includes anti-replay**
 - **Detects and rejects repeated packets**
- **MD5 or SHA-1 can be used**
- **HMAC strengthens the algorithm**

IPSec AH

Original IP datagram



Authenticated IP datagram

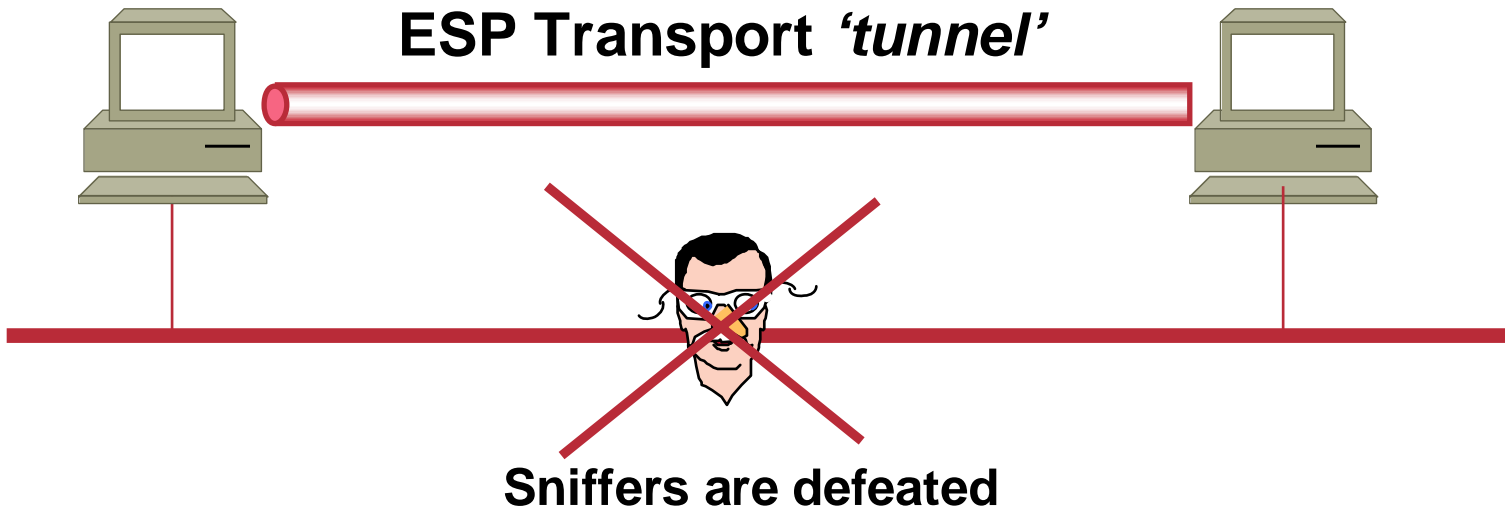
IPSec Encapsulating Security Payload (ESP)

Cisco.com

- **RFC 2406 (Nov '98)**
- **Confidentiality of**
 - **Whole IP datagram (tunnel mode)**
 - **IP payload only (transport mode)**
- **DES (RFC 2405) 3DES (RFC 2451) encryption algorithms can be used**
- **Version 3 IETF draft adds AES (FIPS 197)**
 - **New standard**
 - **More computationally efficient**
 - **Longer keys = more secure**

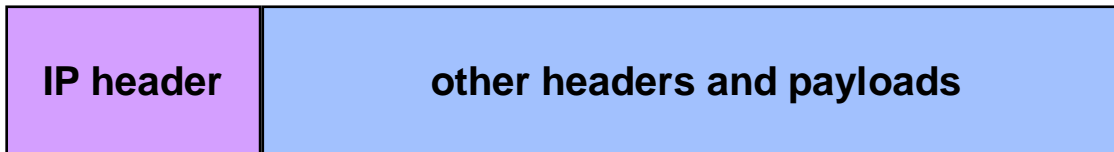
IPSec ESP Transport

- Used end to end, between hosts
- Protects the IP payload only



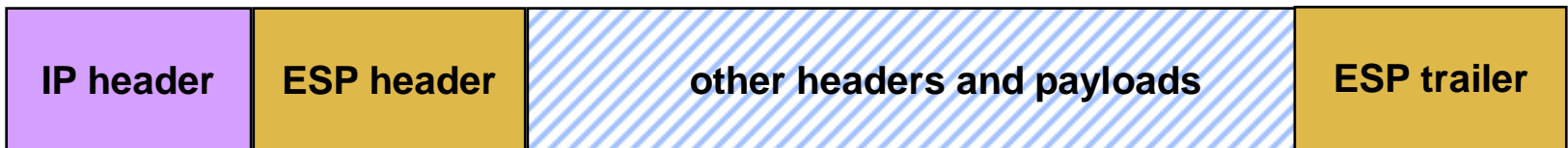
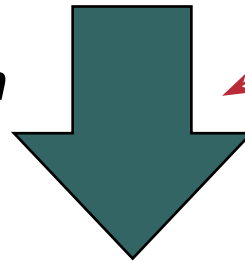
IPSec ESP Transport

Original IP datagram



secret key

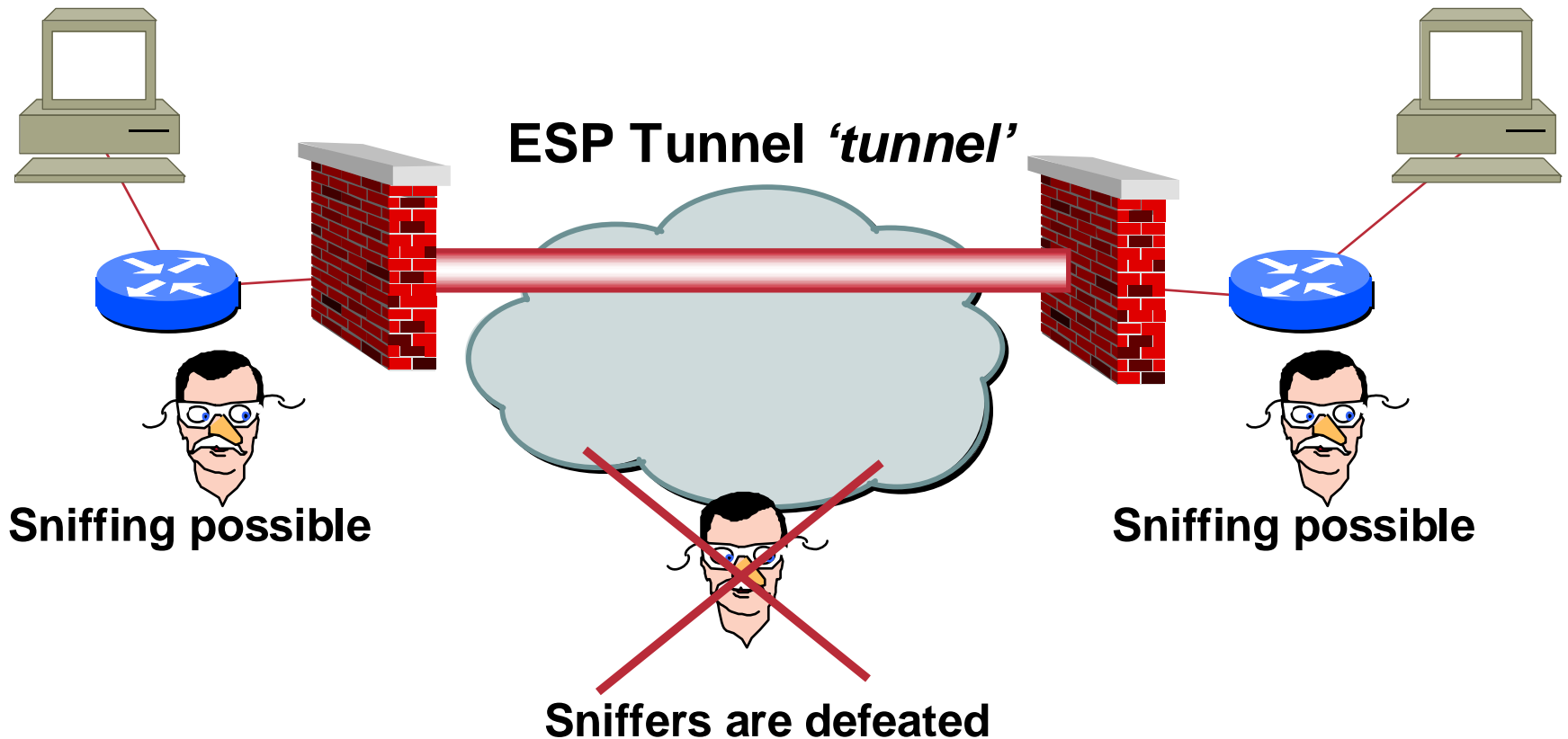
Encryption algorithm



IP datagram with transport ESP

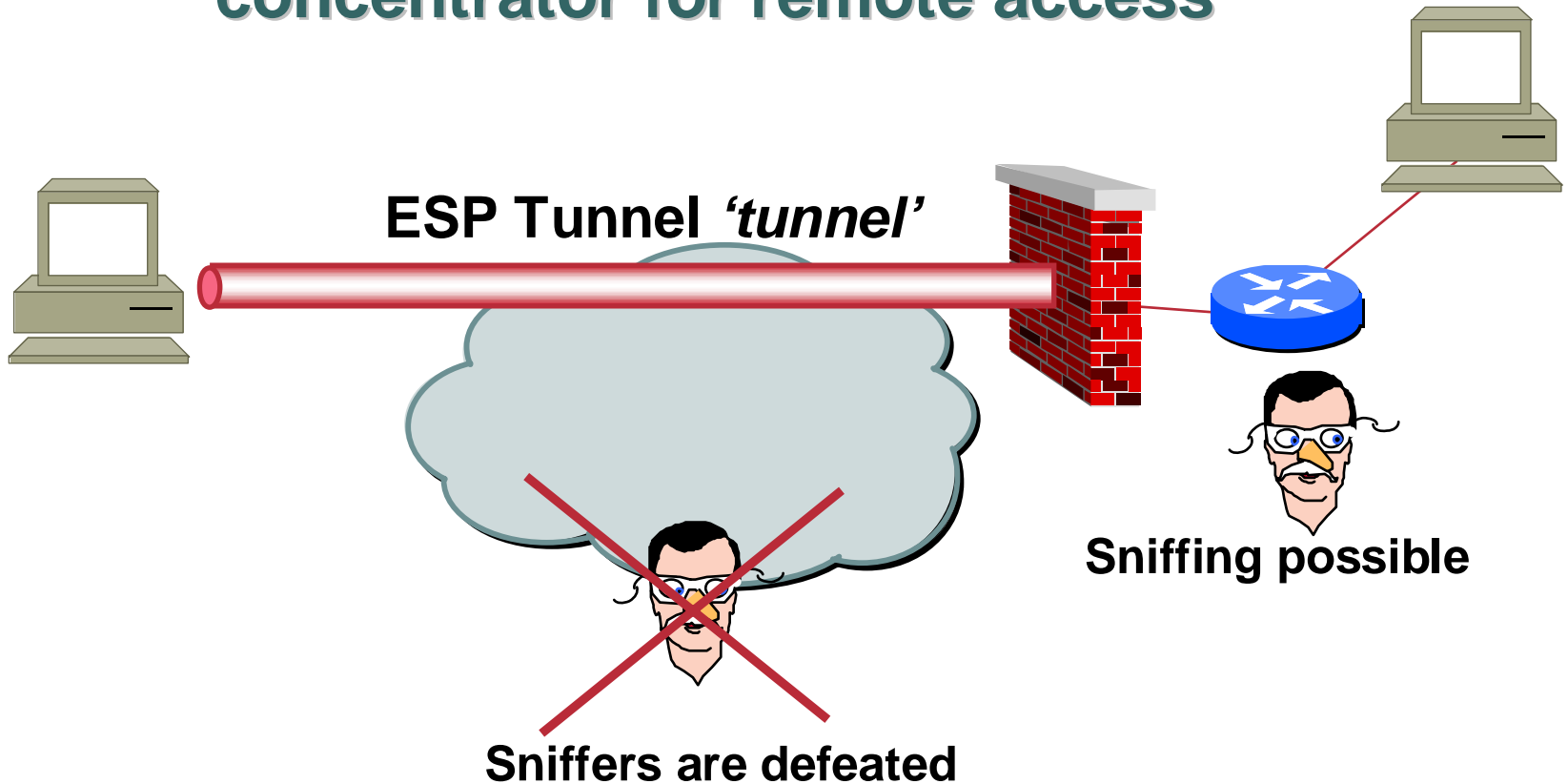
IPSec ESP Tunnel

Usually between firewalls/routers for VPNs



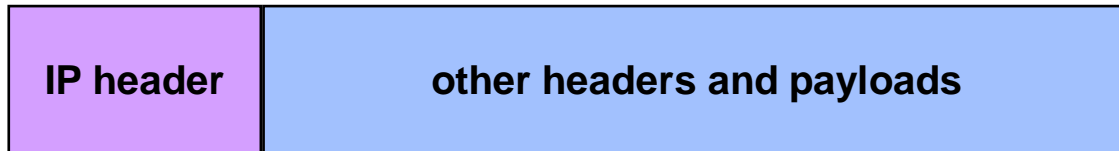
IPSec ESP Tunnel

....or between client and firewall/VPN concentrator for remote access

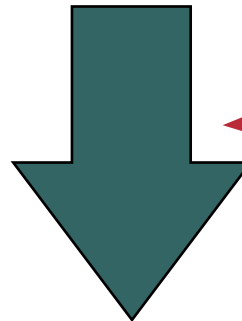


IPSec ESP Tunnel

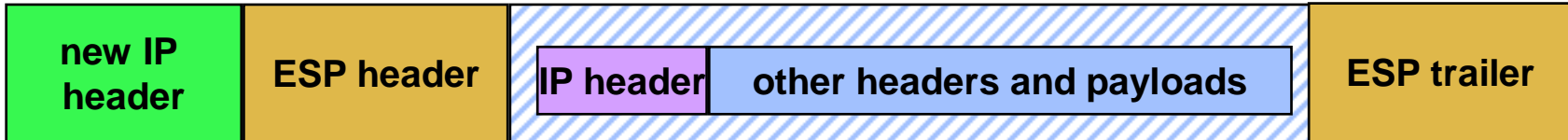
Original IP datagram



New IP header built by tunnel end



Encryption algorithm



IP datagram with tunnel ESP

- **IPSec technologies**
 - Encapsulation types
 - IKE**
 - Encryption
 - Key management
 - Digital certificates

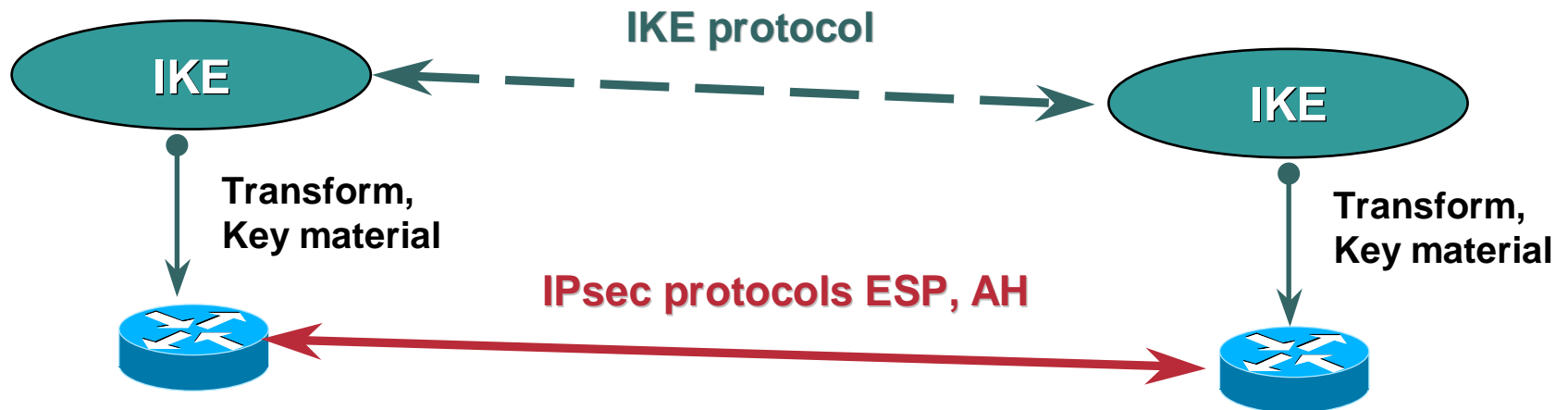
Security Associations



- **Policy agreement between two entities, including:**
 - Encryption algorithm (DES or 3DES)
 - Hash (MD-5 or SHA)
 - Authentication (RSA signature, RSA nonce or pre-shared keys)
 - D-H Group
 - Key lifetime
- **Types of security associations**
 - Bidirectional for management (IKE SA)
 - Unidirectional for data (IPSec SA)

IPSec needs IKE

- Internet Key Exchange (IKE) – RFC 2409
- Negotiates the **IPSec SA policy**
- Eliminates need for manual config of parameters
- Permits certificate authority support



- **IPSec technologies**

 - Encapsulation types

 - IKE

 - Encryption**

 - Key management

 - Digital certificates

Encryption

- **Symmetric Cryptography**

- Uses a shared secret key to encrypt and decrypt transmitted data

- Data flow is bidirectional

- **Provides data confidentiality only**

- Does not provide data integrity or non-repudiation



- **Asymmetric Cryptography**

- Also known as Public Key Cryptography

- Utilizes two keys: **private** and **public** keys

- Two keys are mathematically related but different values

- **Computationally intensive**

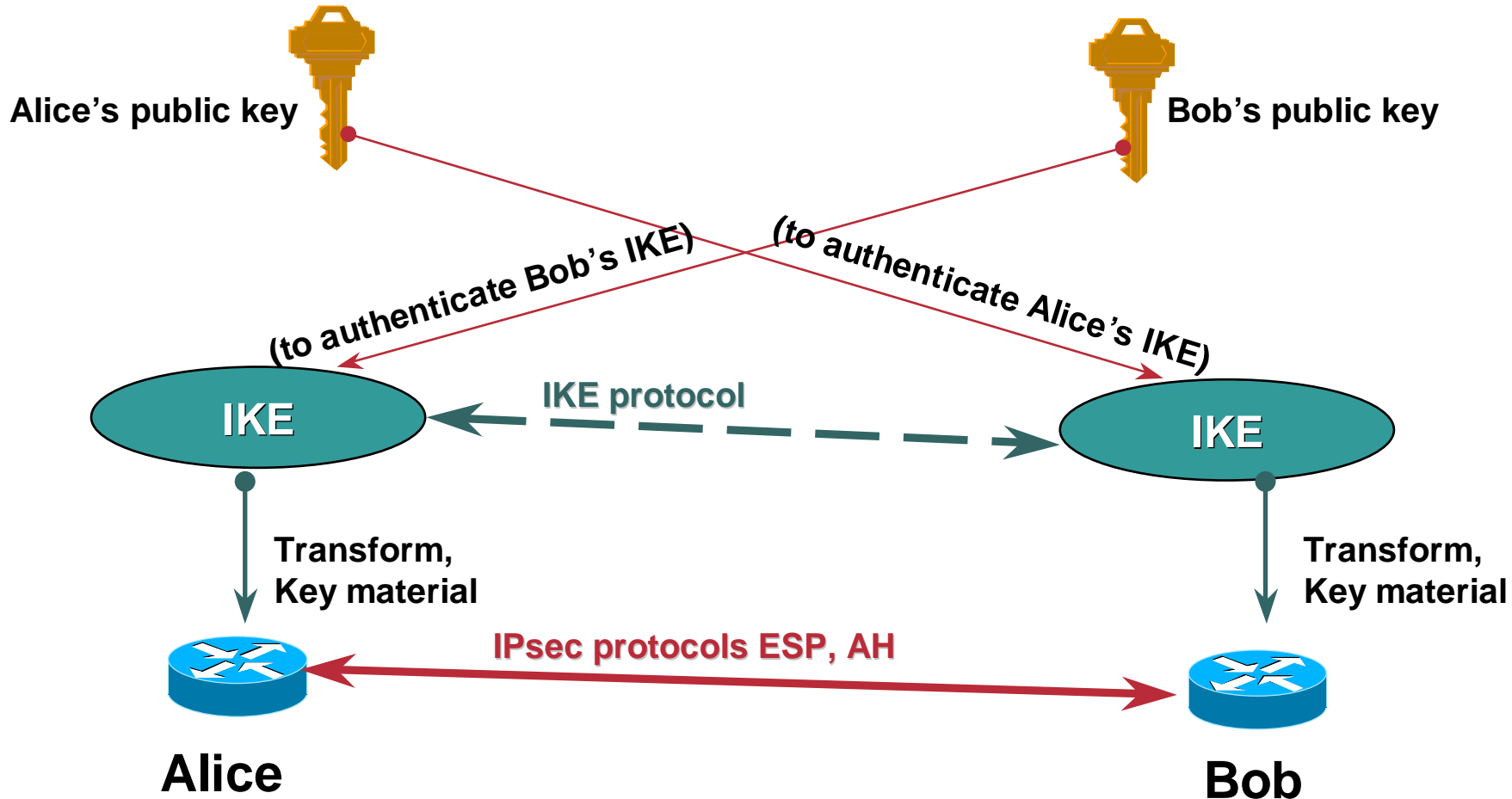
- **Provides data confidentiality**

- Can provide for data integrity as well as non-repudiation



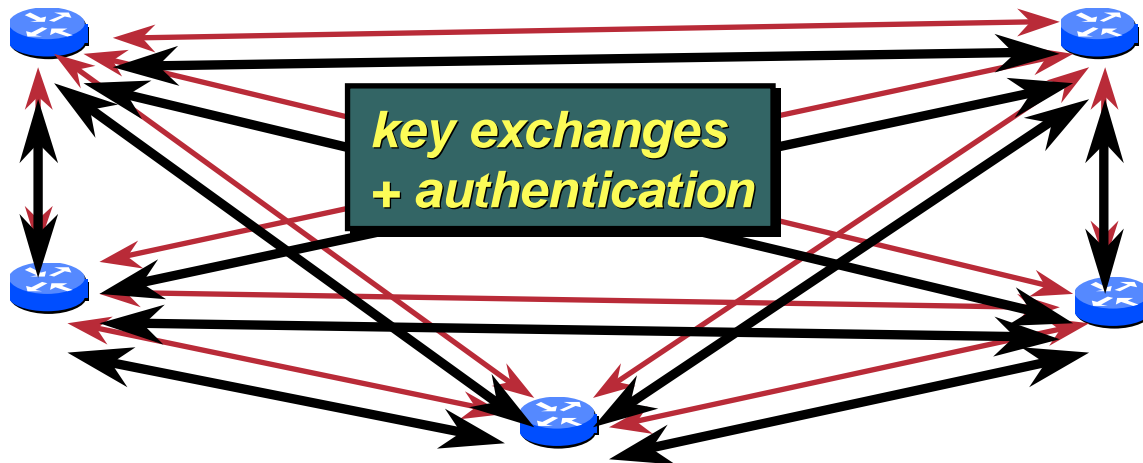
- Definition of IPSec VPNs
- **IPSec technologies**
 - Encapsulation types
 - IKE
 - Encryption
 - Key management**
 - Digital certificates
- IPSec VPN Implementation
- Product Positioning

IKE needs public key authentication



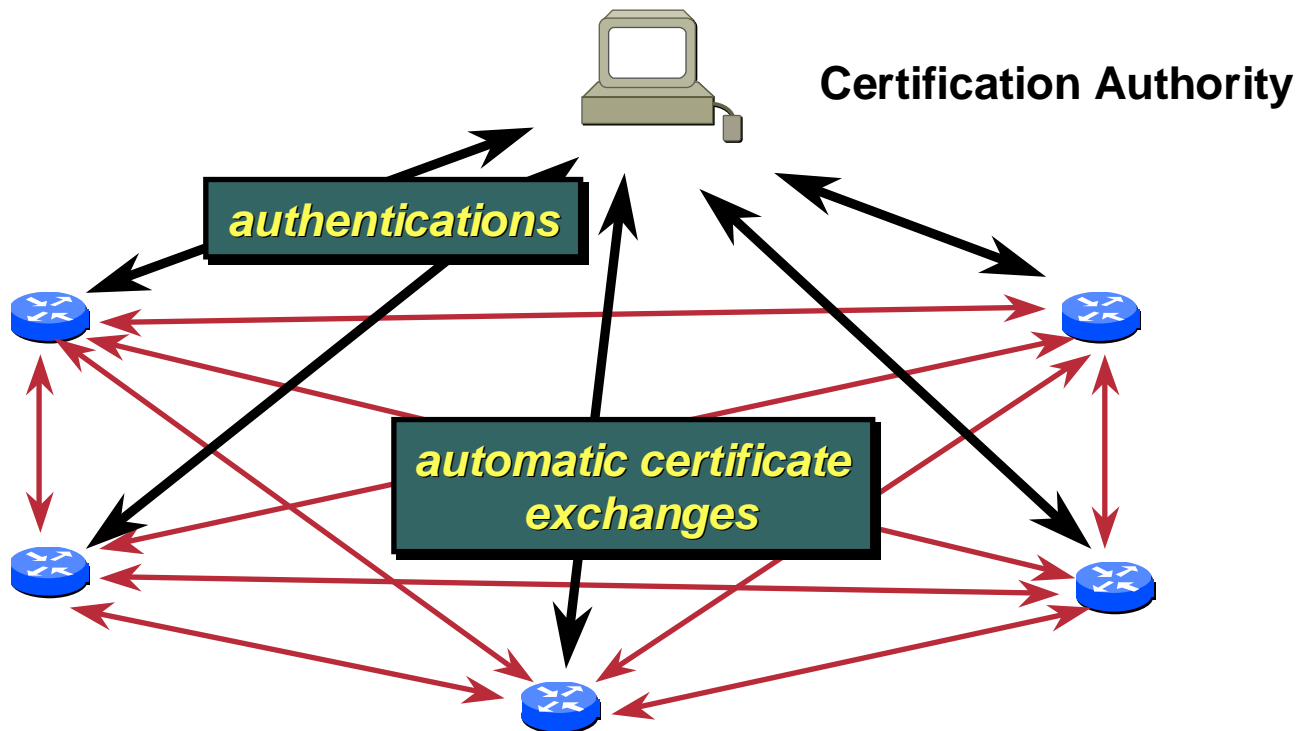
Manual Public Key Exchange cont'd

- **Limited scalability: n peers $\Rightarrow n*(n-1)$ manual key exchange/authentication configs**



Automated Public Key Exchange cont'd

- **Scalable: n peers \Rightarrow n authentication and n certificates**



- **IPSec technologies**
 - Encapsulation types
 - IKE
 - Encryption
 - Key management
 - Digital certificates**

Digital Certificates

- **Can prove that:**

The sender is really who they claim to be

- **Certificates provide scalable authentication**

- **Non Repudiation**

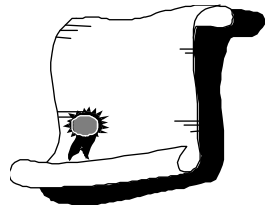
Prevents a party involved in a communication from later denying having participated

Proof of identity of sender

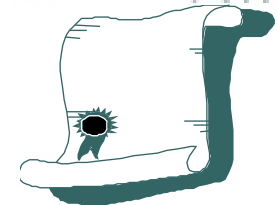
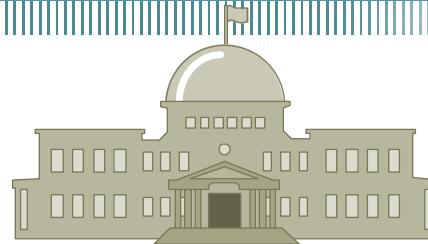


0000123
SHA, DH, 3837829...
1/1/93 to 12/31/98
Alice Smith, Acme Corp
DH, 3813710...
Acme Corporation, Security Dept.
SHA, DH, 2393702347...

How peers work with CA ?



CA's own certificate signed by CA



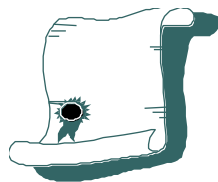
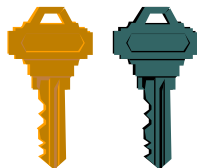
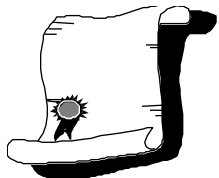
4. Peer's certificate signed by CA

SCEP

2. Peer fetches CA's certificate

3. Peer transmits its public key

5. Peer fetches its certificate



1. Peer generates public/private key pair

Strong or human authentication needed for steps 1. and 2.



Site to Site VPN

IPsec based

Cisco.com

Advantages

- Open standard (multi-vendor support)
- Security (Authentication, Integrity, confidentiality, Authorization)
- Supports large variety of Authentication and Encryption standards
- Quick deployment (no infrastructure changes required)
- Hardware based encryption /decryption available to help address performance and scalability issues
- Some (layer 2 and 3) QoS

Limitations

- The overlay point-to-point mesh required leads to N-squared scalability issues
- Performance and scalability are hindered by computationally intensive encryption / decryption
- Can become costly to implement (Certificate Authorities and Key Management services, hardware upgrades for encryption acceleration, software upgrades, etc.)
- Export restrictions on encryption technology
- Only supports tunneling of IP packets
- Adding new sites imply VPN complex reconfiguration
- No support of intra-VPN routing
- No support of IP Multicast

IPsec VPN: when to use?

- Need to build a secure, partially meshed Intranet/Extranet.
- Allow secure access for mobile users
- Support hub-and-spoke non-hierarchical topology
- Support of private addressing RFC1918
- Standard RFC-based solution
- Use of Certificates

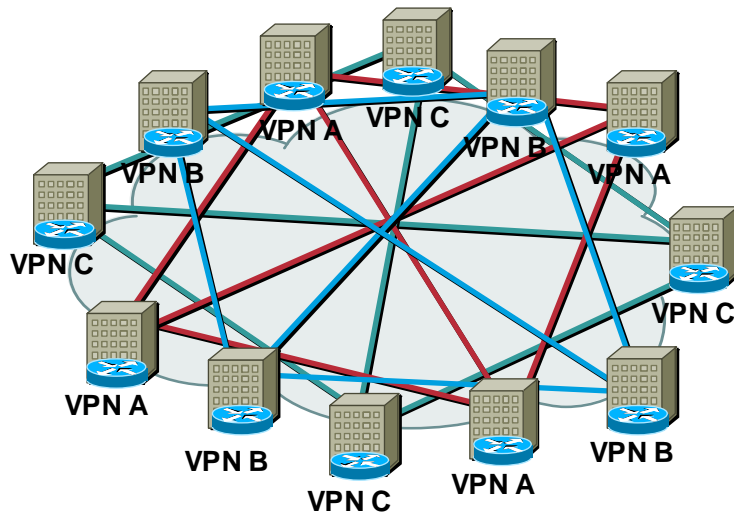
Site to Site, MPLS Based VPN

Multiprotocol Label Switching (MPLS)

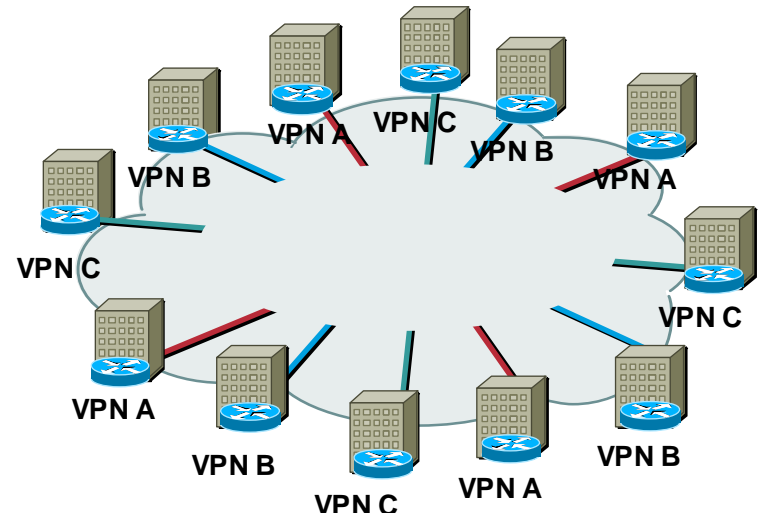
- **MPLS characteristics:**
 - **Packet classification only where the packet enters the network**
 - **Packet classification is encoded as a label**
 - **Packets are forwarded in the core, without having to re-classify them - No further packet analysis**
 - **Label swapping - packets are switched, not routed**

Overlay VPNs vs. MPLS VPNs

VPN Topology



Connection-Oriented



Connectionless

VPN Aware Network :
VPNs are “built-in” rather than “overlaid”

Site to Site VPN

MPLS

Advantages

- Open standard
- Flexible architectures extend IP services over multiple technologies (e.g. IP + ATM)
- Centralized provisioning and management
- Cisco IOS combines all VPN-enabling technologies (MPLS, BGP, QoS features, etc.)
- Compatible with other VPN technologies (IPsec, PPP tunneling, etc.)
- Enables non-VPN related features:
 - Traffic engineering (RRR)
 - Faster packet switching through network (label switching > packet routing)
 - Making ATM network IP-aware
- Transparent to Intra-VPN Routing
- Easiness in adding|move sites
- No need of complex CPE configuration

Limitations

- Likely requires software and protocol upgrades of SP's IP network
 - Multiprotocol extension for BGPv4,
 - Provisioning PE functionality on Edge LSRs, IP / MPLS / ATM QoS/CoS mapping,
 - Usage Monitoring
 - SLA enforcement
 - Billing setup, etc.
- Security
 - No Integrity
 - No confidentiality
- Single SP (not over Internet), no IPMc

MPLS VPN: when to use?

- **MPLS-VPN enabled Public IP Network (SP)**
- **Need to build a full-meshed Intranet/Extranet.**
- **Support of private addressing RFC1918**
- **Standard based solution**
- **Ease of VPN re-configuration/provisioning**
- **Provides scalable, robust QoS mechanism**
- **Traffic engineering capabilities**

Recap

Recap: Ways to Build IP VPNs

- IP based infrastructure with tunnelling
- Frame relay with virtual circuits
- Multi Protocol Label Switching
Forwards packets based on Labels

Connection based



IP/IPsec/L2TP Tunnel

The diagram shows a yellow cloud representing a network. Inside the cloud, a red horizontal bar with a gradient and a drop shadow contains the text 'IP/IPsec/L2TP Tunnel'.



Private Virtual Circuit

The diagram shows a grey cloud representing a network. A red dotted line forms a path across the cloud, representing a virtual circuit.

Connectionless



Data Data Data Data

The diagram shows a grey cloud representing a network. Inside the cloud, four small colored boxes (pink, teal, pink, green) are arranged horizontally, each containing the word 'Data'.

Recap: VPN Services

	L2TP	GRE	IPsec	MPLS
Authentication	X		X	
Integrity			X	
Confidentiality			X	
RFC 1918	X	X	X	X
Intra-VPN rout.		X	X*	X
QoS	X	X	X	X
Non IP Protocols	X	X		
Scalability	X			X
Application	RA, Extranet	Intranet	RA, S2S	Intranet

CISCO SYSTEMS



EMPOWERING THE
INTERNET GENERATION