Course: Computer Networks V
Autumn 2010

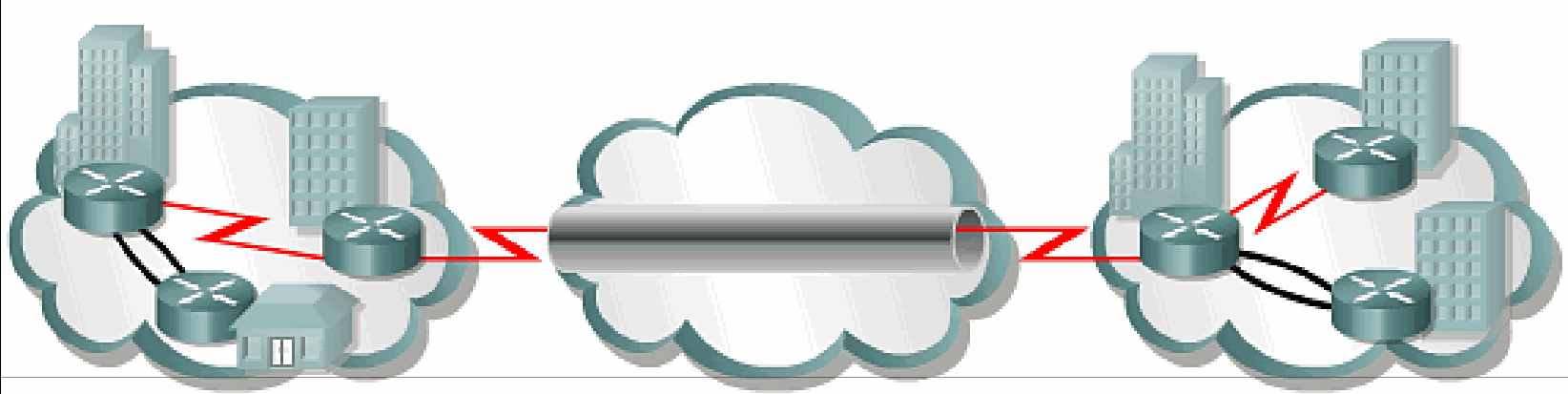
Philip Heimer
philip.heimer@hh.se

VIRTUAL PRIVATE NETWORKS

What is a VPN?

- ***A Virtual Private Network (VPN) is*** defined as network connectivity deployed on a shared infrastructure with the same policies and security as a private network.

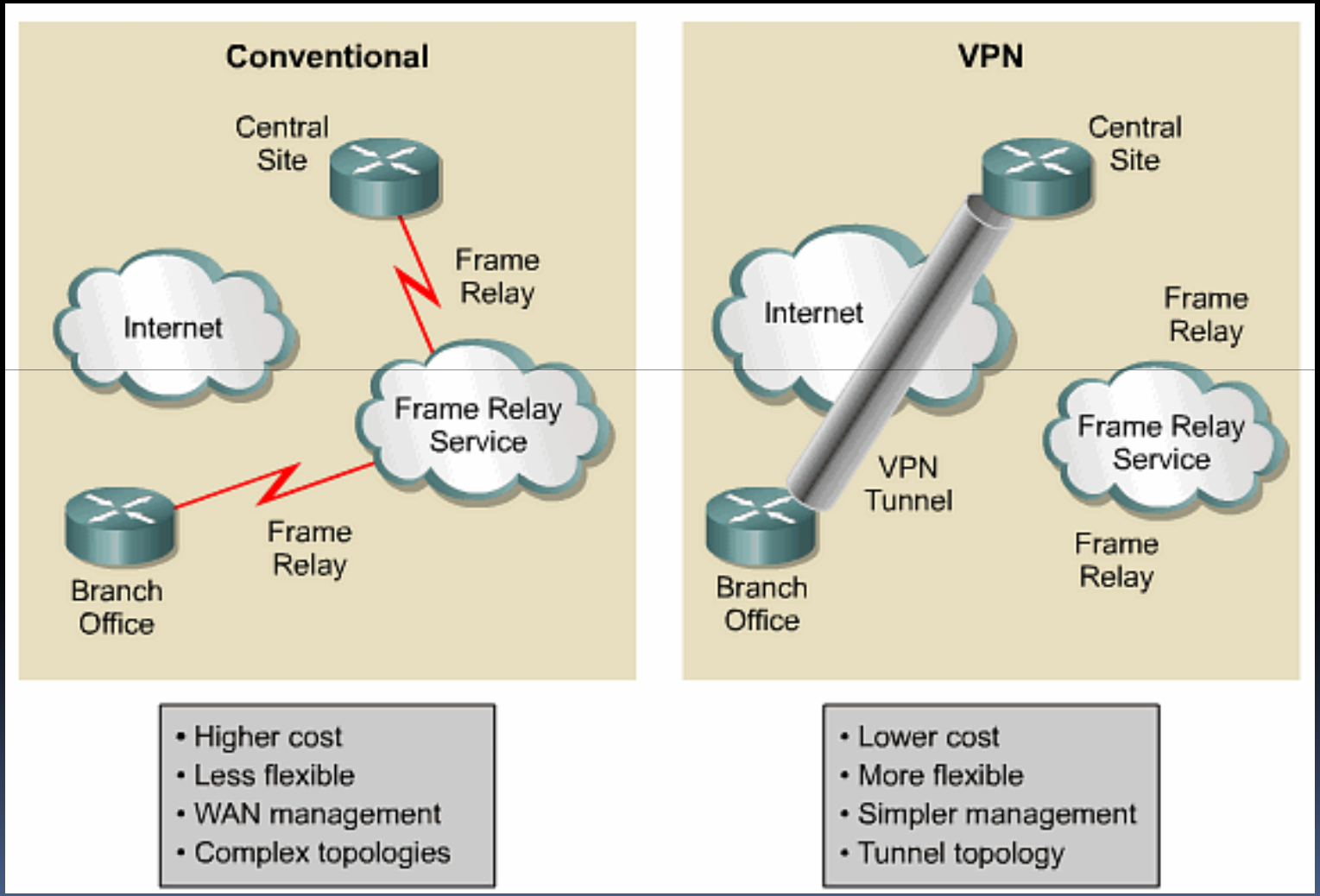
Virtual Private Networks



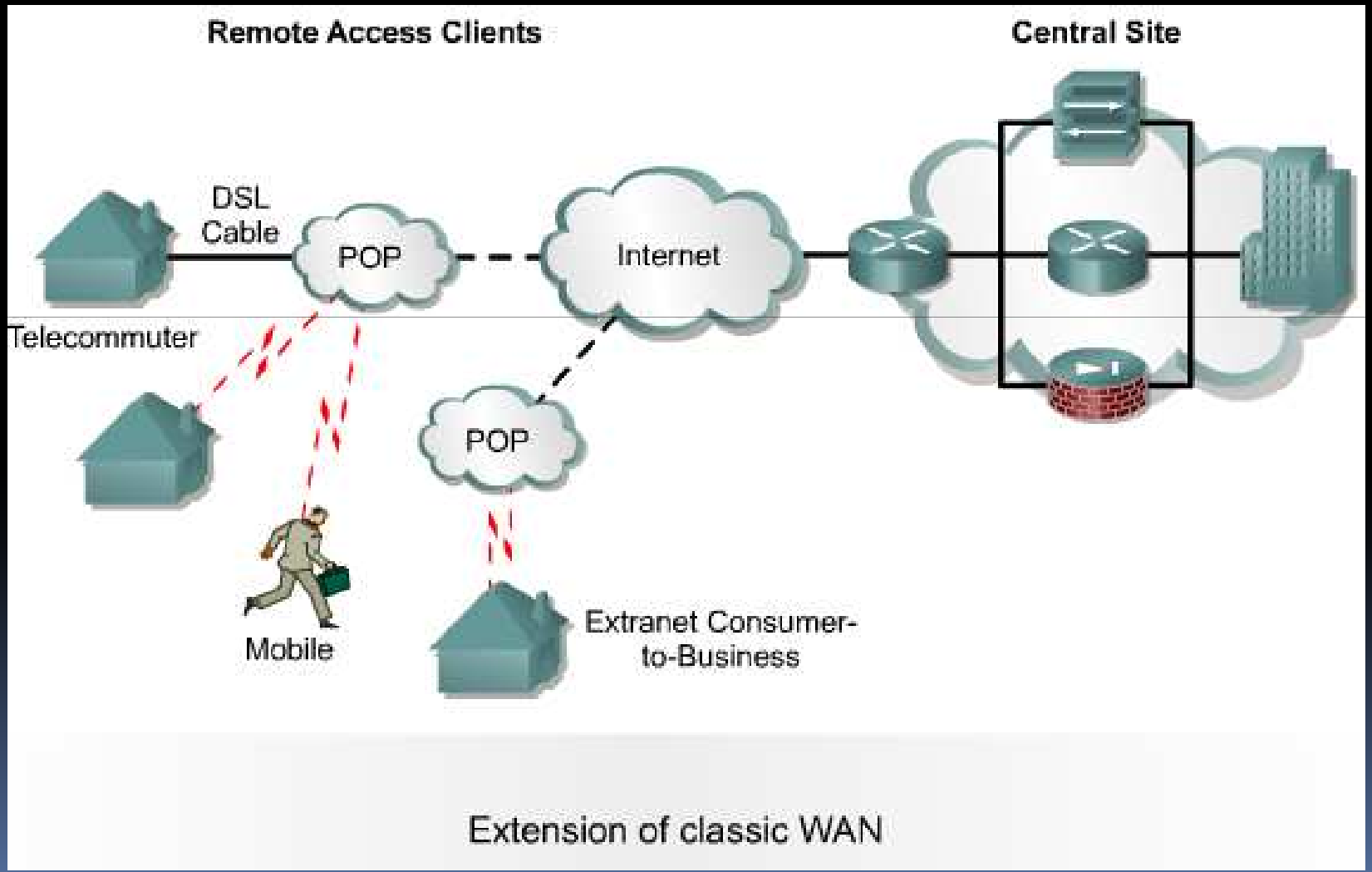
A VPN carries private traffic over a public network using advanced encryption and tunnels to protect:

- Confidentiality of information
- Integrity of data
- Authentication of users

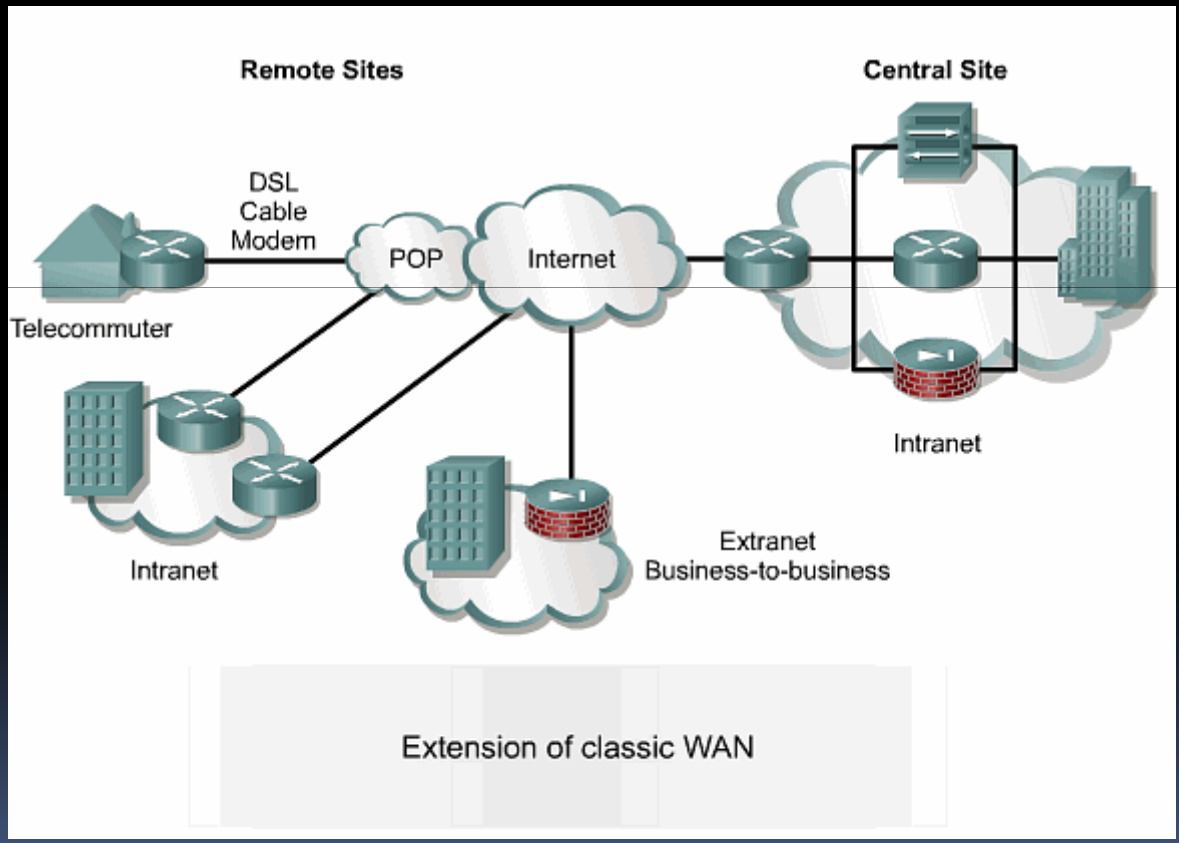
Why have VPNs?



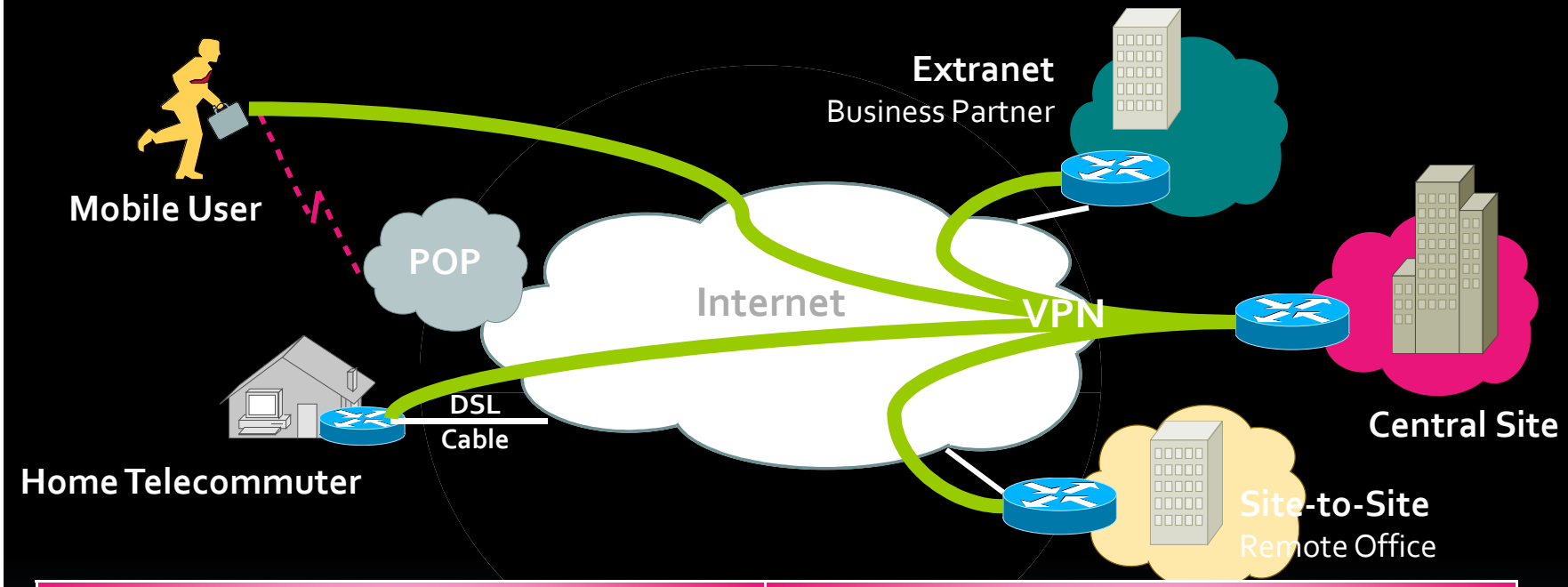
VPN Types
Remote Access VPN Solutions



Site-to-Site VPN Solutions



VPN Requirements Vary By Application



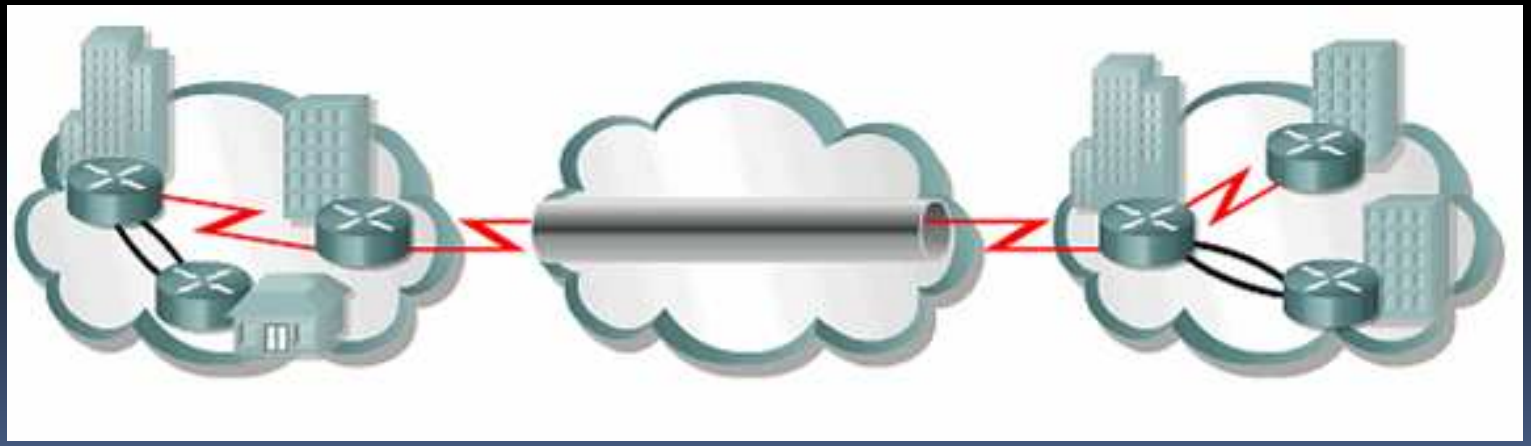
Remote Access VPN	Site-to-Site VPN
• Evolution away from dial • Per-user manageability • Multi-OS (desktop) support • Deployment scalability	• Extension of classic WAN • Compatibility with diverse network traffic types • Integration with routing • Deployment scalability

Different types of VPN-protocols

VPN Protocols	Description	Standard
L2TP	Layer 2 Tunneling Protocol	RFC 2661
GRE	Generic Routing Encapsulation	RFC 1701 and 2784
IPSec	Internet Protocol Security	RFC 2401

IPSec – IP Security

- Authentication
- Data Integrity
- Confidentiality
- Anti-replay



The IPSec suite

- IPSec contains a bunch of protocols that allows for it to manage the different types of security mentioned on the previous slide.
- Negotiation protocol: IKE – Internet Key Exchange
  - -Allows devices to negotiate what kind of setup they want. They may use a combination of the following:
- Security protocol : AH, ESP, ESP+AH
- Encryption: DES, 3DES, AES
- Authentication: MD5, SHA-1
- Protection: DH1, DH2, DH3

AH and ESP

Authentication Header

- Ensures data integrity
- Provides origin authentication - ensures packets definitely came from peer router
- Uses keyed-hash mechanism
- Does NOT provide confidentiality (no encryption)
- Provides optional replay protection

Encapsulating Security Payload

- Data confidentiality (encryption)
- Limited traffic flow confidentiality
- Data integrity
- Optional data origin authentication
- Anti-replay protection
- Does not protect IP header

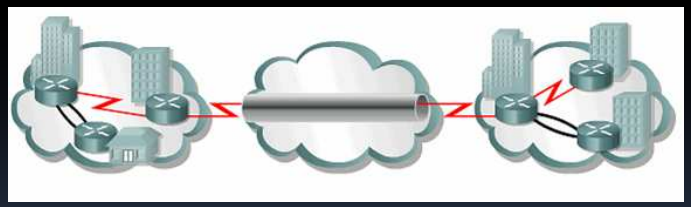
Modes of communication

- Transport mode

DATA	ESP	IP	L2

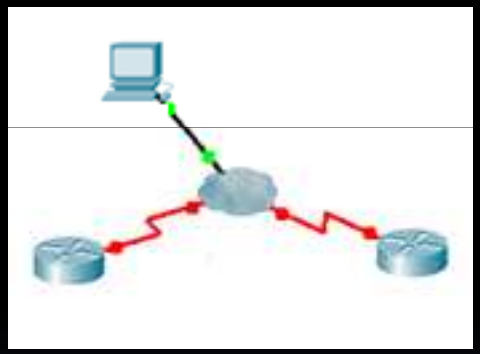
- Tunnel mode

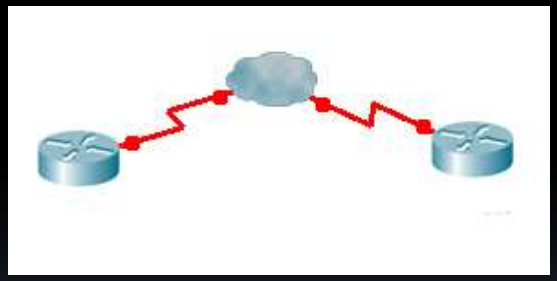
DATA	IP	ESP	IP	L2



How you may authenticate to IPSec VPN

- Remote access connections may use username & password, one-time passwords or biometrics.



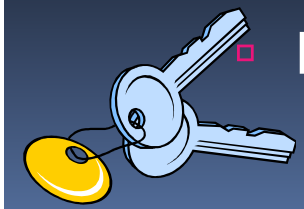


- Site –to –site connections
  - Devices may use pre-shared keys or certificates.

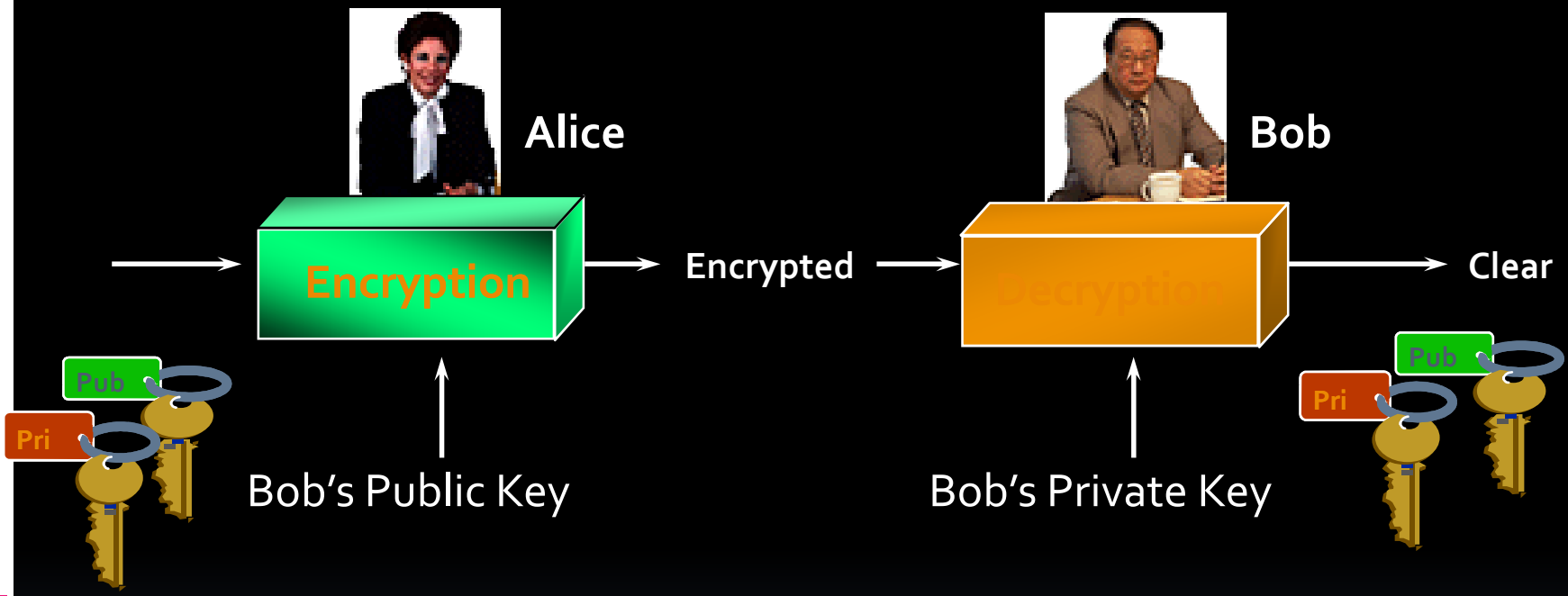
Encryption –Symmetric and asymmetric keys

- Symmetric – Each peer uses the same key to encrypt and decrypt data. (Used to create shared secret keys)

- Asymmetric – A peer uses one key to encrypt and another key to decrypt data. (“Unbreakable” keys)
  - Public key – Private key – Encrypt – Decrypt.



RSA or Diffie-Hellman kind of encryption – (Asymmetric)



- Alice gets Bob's public key
- Alice encrypts message with Bob's public key
- Bob decrypts message using his private key

DH & RSA encryption values

- DH group 1: 768-bit group creates the key
- DH group 2: 1024-bit group creates the key
- DH group 5: 1536-bit group creates the key

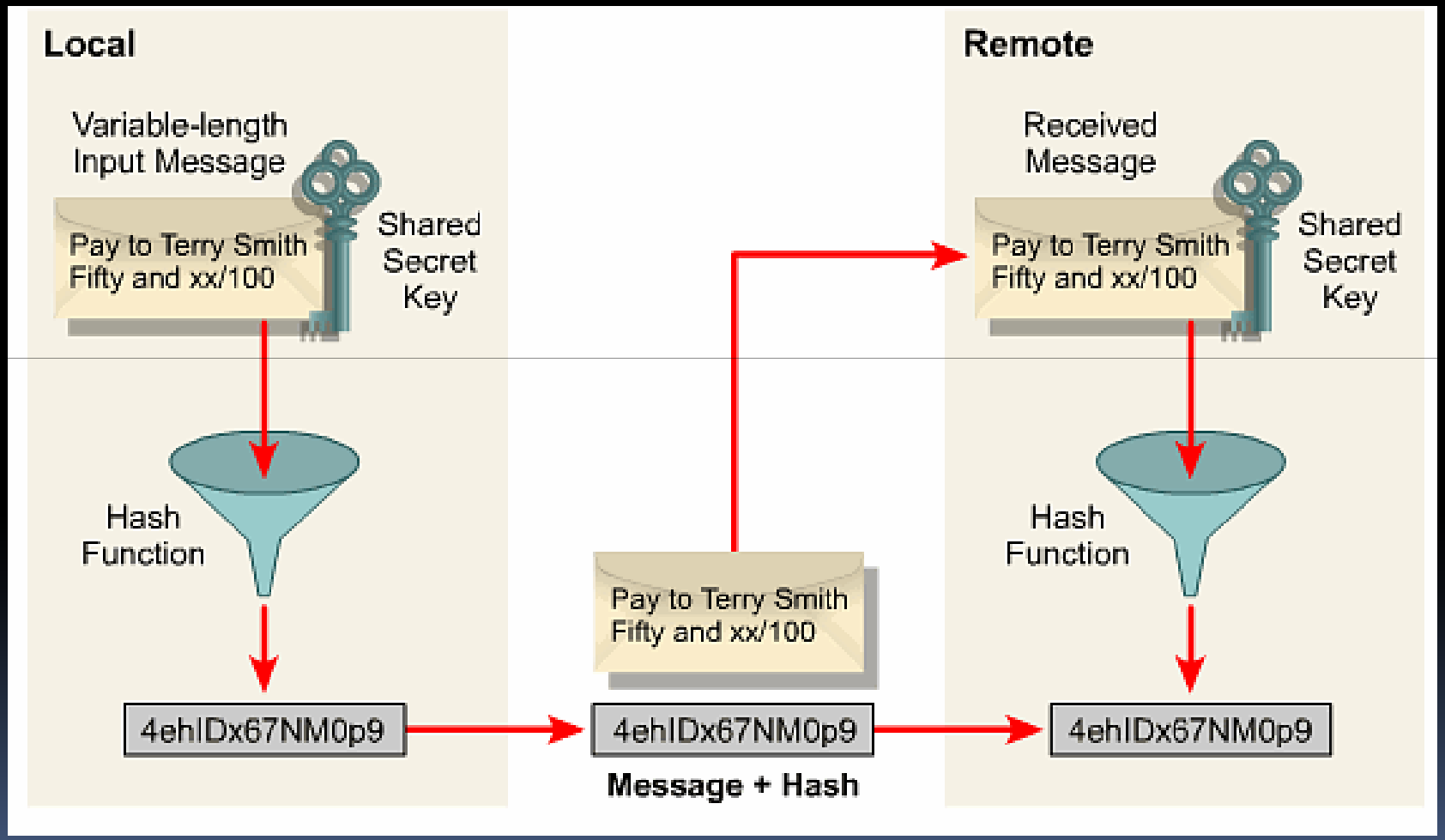
- Each bit added doubles the encryption strength(!)

- RSA (Rivest, Shamir & Adleman) may come in the values of 512-, 768-, 1024-bit or larger values.
- Used for misc. encrypting such as for sending emails or encrypting telnet sessions. (via ssh-1/2).

Symmetric keys - used as shared secret keys.

- DES
  - – Data Encryption Standard – creates 56-bit key
- 3DES
  - - Uses three DES-keys to create a 168-bit key
- AES (Introduced 2001)
  - - Advanced Encryption Standard – creates 128, 192 or 256-bit key. Newer and more efficient.

Hashing


Local
Remote
Variable-length
Input Message
Pay to Terry Smith
Fifty and xx/100
Shared
Secret
Key
Received
Message
Pay to Terry Smith
Fifty and xx/100
Shared
Secret
Key
Hash
Function
Hash
Function
Pay to Terry Smith
Fifty and xx/100
4ehIDx67NM0p9
4ehIDx67NM0p9
4ehIDx67NM0p9
Message + Hash

IKE phase 1

- 1: Exchange and negotiate policy
  - Send over a list of combinations of algorithms that you would like to use:
    - Ex. Policy 10:
      - Encryption: AES
      - Authentication SHA-1
      - Diffie-Hellman group 2

- 2: Exchange Diffie-Hellman keys. (Public keys) to create a secure medium to send your pre-shared keys across.
- 3: Send pre-shared keys across and verify your identity.

IKE phase 2

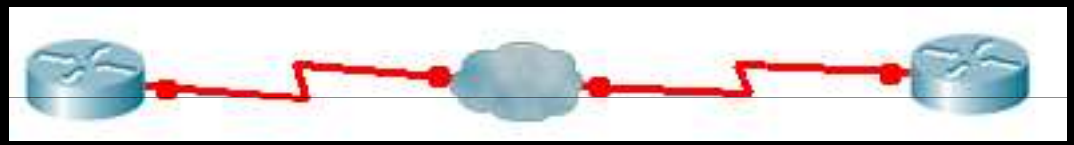
- Exchange symmetric keys to encrypt data for the rest of the session. May be timelimited or based on bandwidth.
  - 64-bit up to 256-bit keys.
- A security association (SA) is formed between the peers.

- Remote users may have to use extended authentication "xauth" on top of the pre-shared keys (or whatever is used) in order to negotiate a session.

Interesting traffic

Define what traffic will be protected by IPSec using an extended access-list.

- Do you remember?



- Sending interesting traffic to the other side will trigger

the peers to negotiate a security association.

May be done using an extended ping

Configuring IPSec through the CLI

- Configure IKE phase 1 using "crypto isakmp" commands.
  - Internet Security and Association Key Management Protocol
    - Create one or more policies to make a secure channel
    - Define pre-shared keys
- Configure IKE phase 2 using "crypto ipsec" commands.
  - Create a transform-set – What symmetric keys , hashing methods and authentication (optional) to be used for the rest of the session.
- Create an access-list to define interesting traffic.
- Create a crypto-map
  - Ties together the transform-set, interesting traffic, IPSec peers and settings such as lifetime to be used for the session.
- Apply crypto-map to an interface.

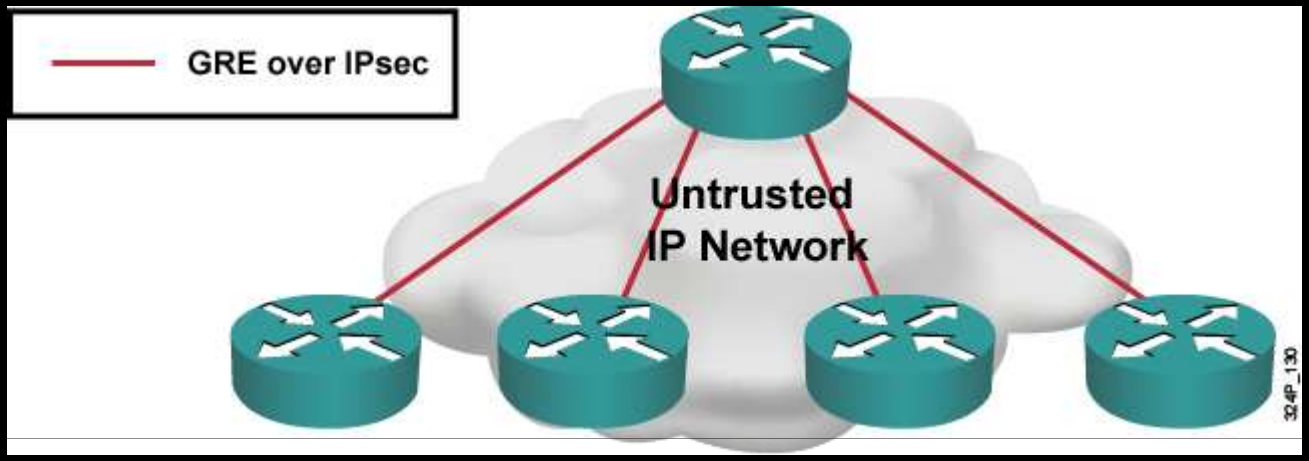
Generic Routing Encapsulation GRE

- GRE is an OSI Layer 3 tunneling protocol:
  - Encapsulates a wide variety of protocol packet types inside IP tunnels
  - Creates a virtual point-to-point link to Cisco routers at remote points over an IP internetwork
  - Uses IP for transport
  - Uses an additional header to support any other OSI Layer 3 protocol as payload (for example, IP, IPX, AppleTalk)

Secure GRE Tunnels

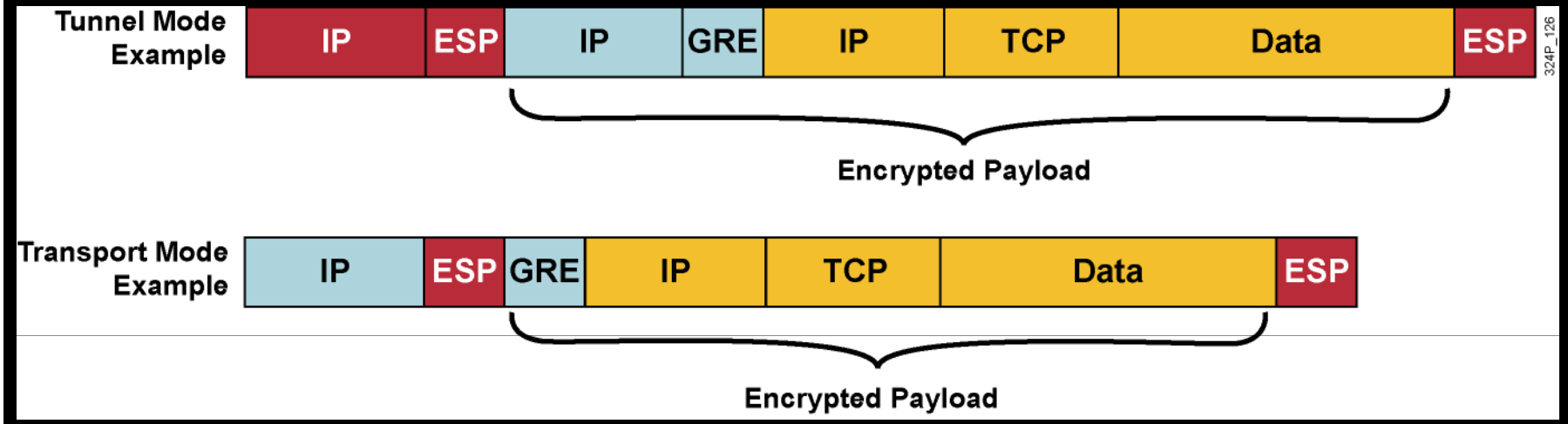
- IPsec provides what GRE lacks:
  - Confidentiality through encryption using symmetric algorithms
  - Data source authentication using HMACs Data integrity verification using HMACs
- IPsec is not perfect at tunneling:
  - Older IOS versions do not support IP multicast over IPsec
  - IPsec was designed to tunnel IP only (no multiprotocol support)
  - Using crypto maps to implement IPsec does not allow the use of routing protocols across the tunnel
  - IPsec does not tunnel IP protocols; GRE does

GRE over IPsec



- GRE over IPsec is typically used to do the following:
  - **Create a logical hub-and-spoke topology of virtual point-to-point connections**
  - **Secure communication over an untrusted transport network (e.g. the Internet)**

GRE over IPsec Encapsulation



- GRE encapsulates an arbitrary payload.
- IPsec encapsulates unicast IP packet (GRE):
  - Tunnel mode (default): IPsec creates a new tunnel IP packet
  - Transport mode: IPsec reuses the IP header of the GRE (20 bytes less overhead than tunnel mode)

Next week

- MPLS+MPLS VPN