NETWORK SECURITY

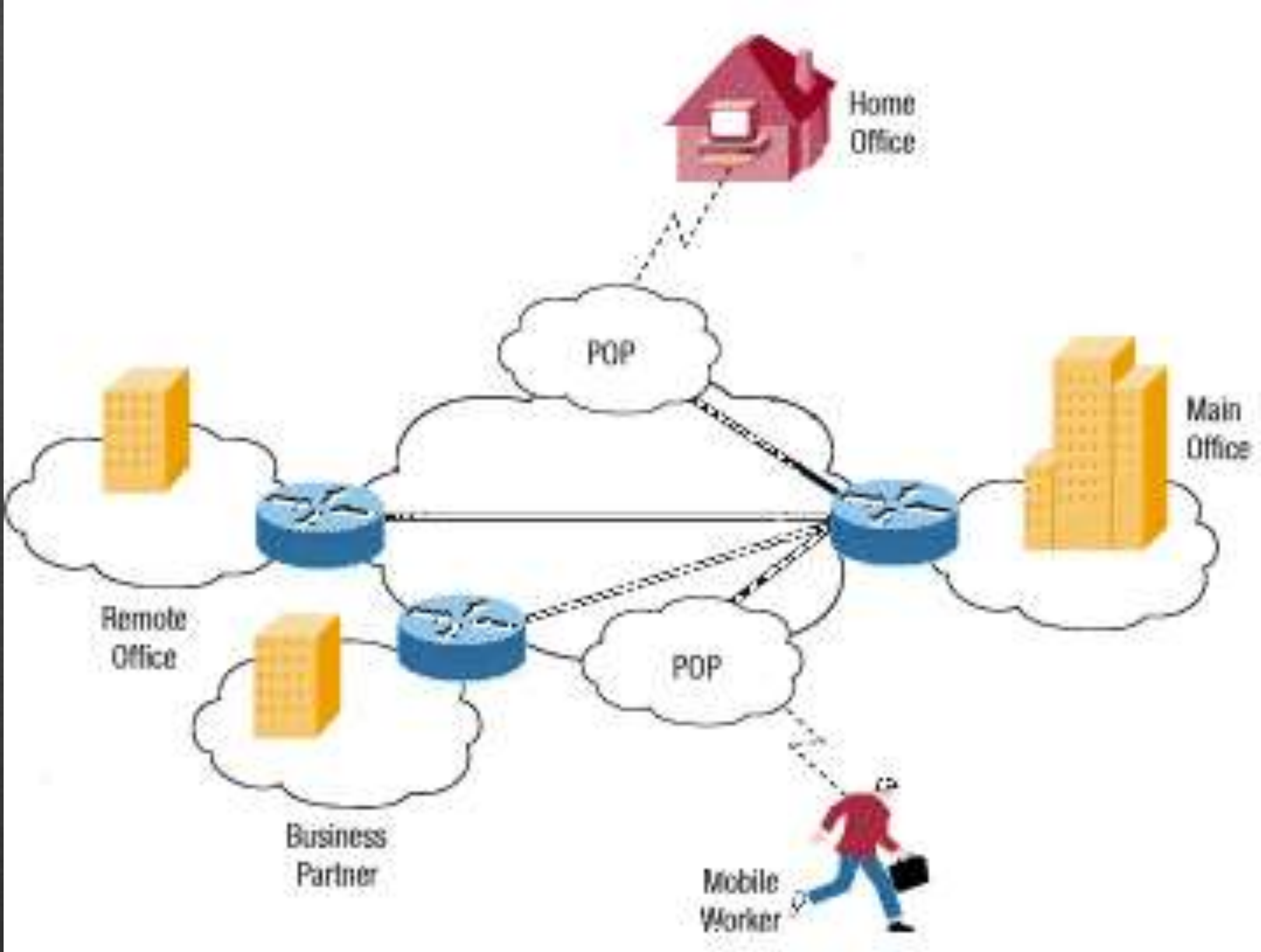
Ch. 11: Virtual Private Network

PTIIK
PROGRAM TEKNOLOGI INFORMASI DAN ILMU KOMPUTER

Goals

- The goal of this chapter is to address
  - the what (what a VPN is),
  - the why (why VPNs are popular),
  - (how VPNs provide secure communications) of VPNs

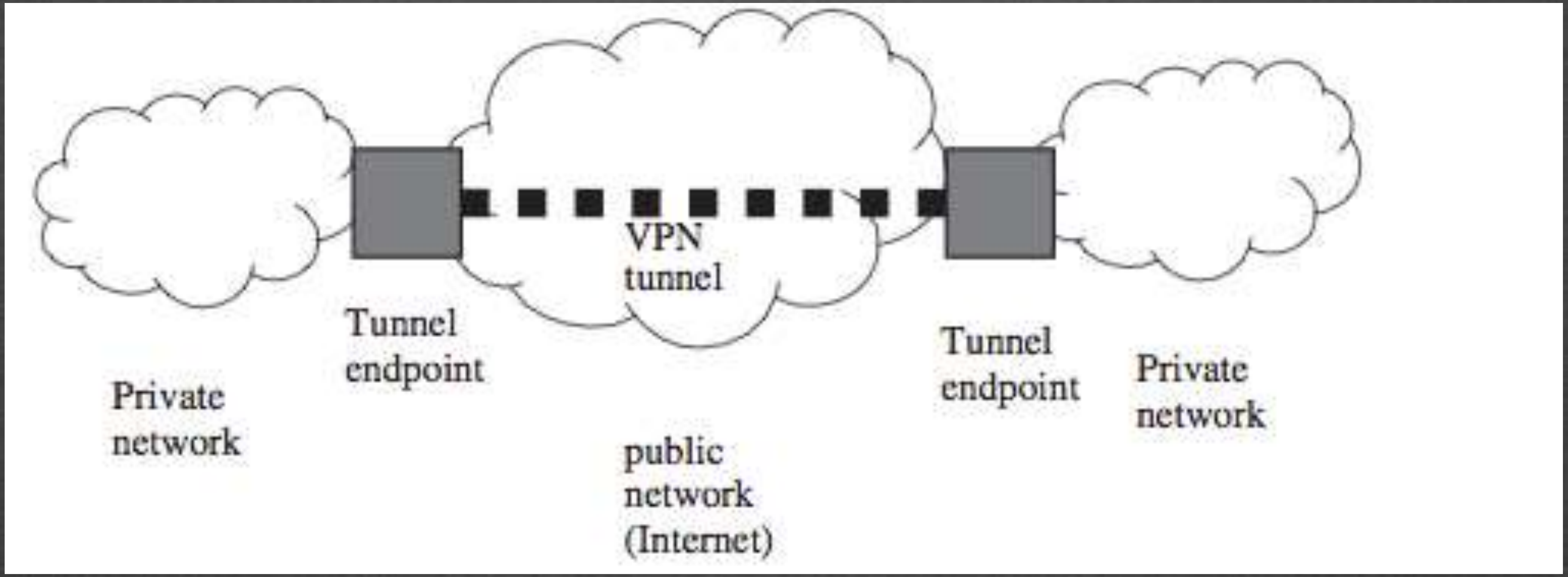
How VPN work


Home Office
POP
Main Office
Remote Office
POP
Business Partner
Mobile Worker

VPN

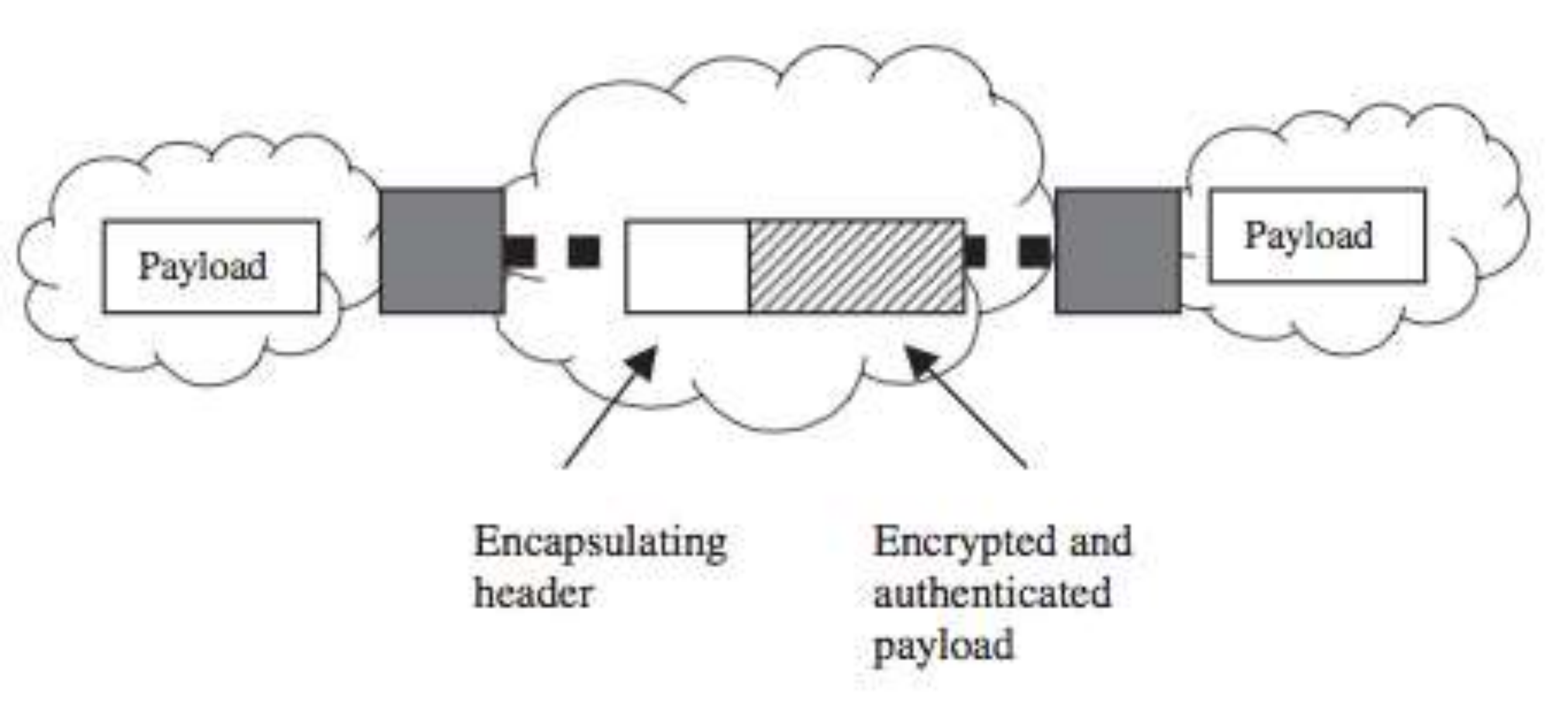
- A VPN provides a mecha- nism by which two networks can communicate with each other over a public infrastructure, such as the Internet, by tunneling the data in a way that emulates a logical point-to-point connection
- A VPN can be defined as a network that provides a secure link between two private networks

Basics of VPN Configuration and Operation



- The network is virtual (emulating a logical point-to-point connection)
- The network is private because the tunnel provides data confidentiality, integrity, authentication, and access control

Concept of A Secure Tunnel Mechanism



- The payload is encapsulated with a new header by the tunnel endpoint when it enters the tunnel and de-encapsulated when it leaves the tunnel

VPN BENEFITS

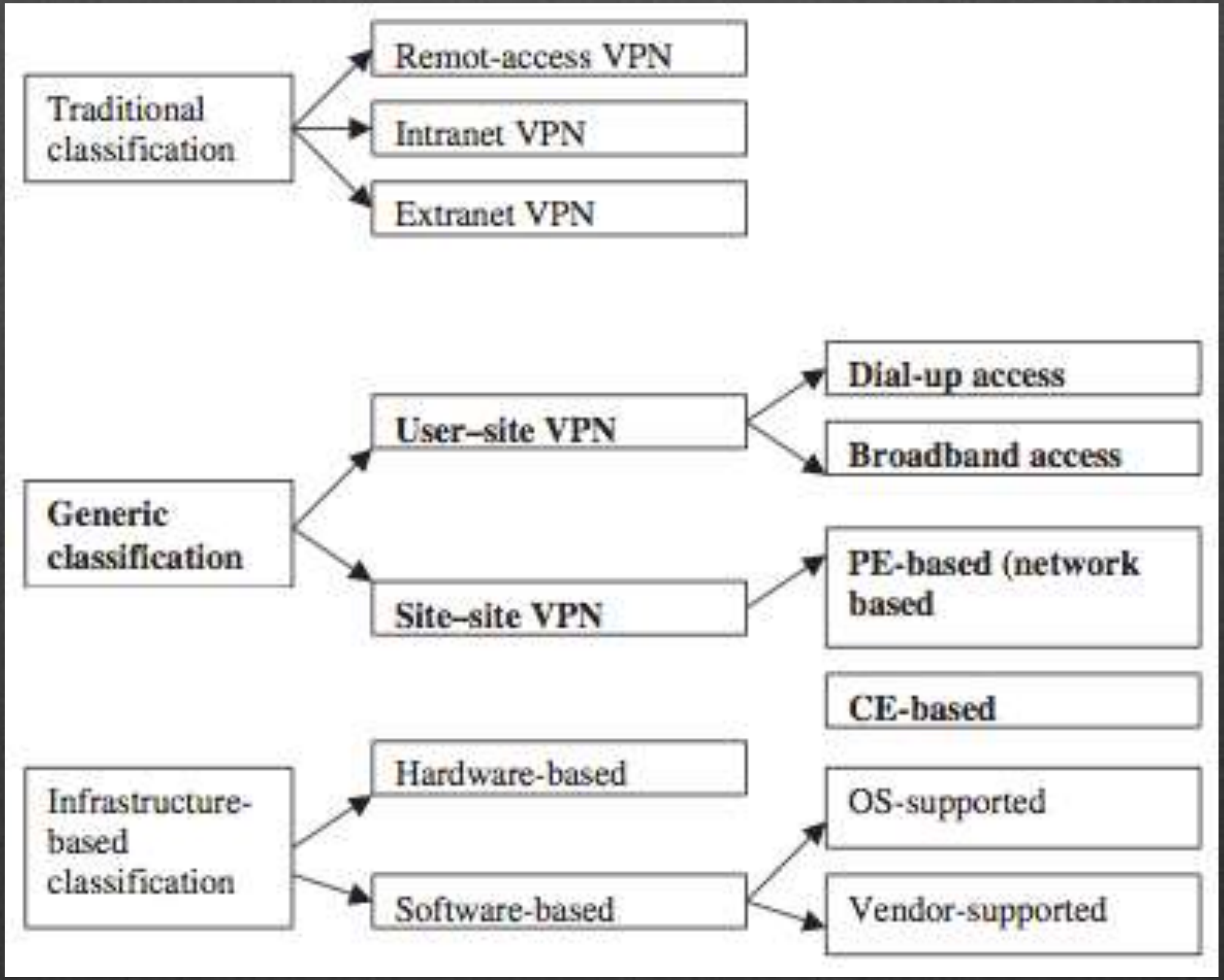
- Cost Savings
- Scalability
- Flexibility

VPN TERMINOLOGIES

- VPN Client.
- VPN Server.
- VPN Tunnel
- Tunnel Endpoints
- Tunneling Protocol
- P (Provider) Network and C (Customer) Network
- P Devices and C Devices
- PE (Provider Edge) Devices and CE (Customer Edge) Devices
- VPN Concentrator

VPN TAXONOMY

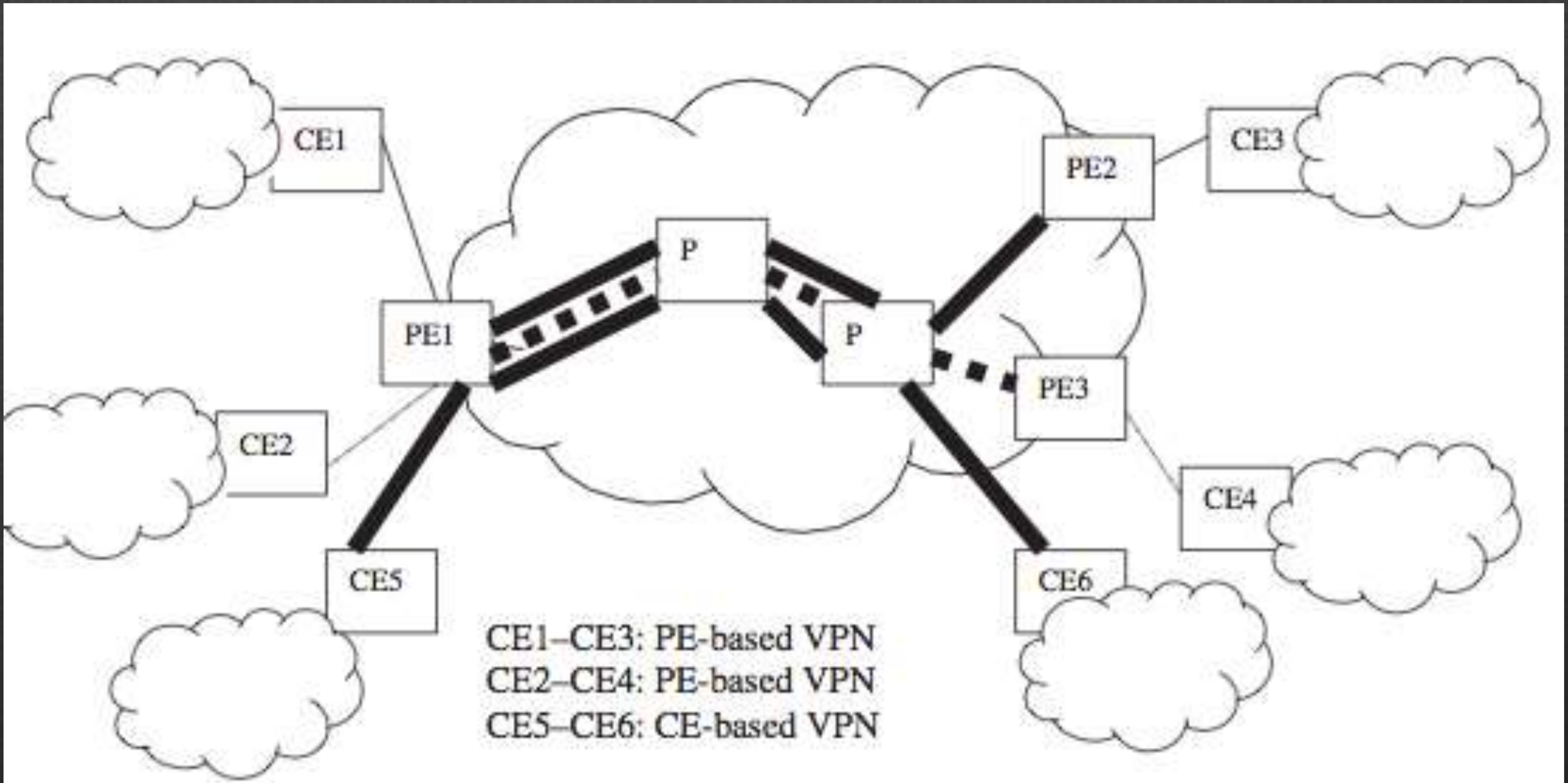
- Traditionally, VPNs have been classified into remote access, Intranet, and Extranet VPNs



Tunnelling Modes

- –The ISP’s access server intercepts the remote user’s PPP connection and builds a tunnel to the corporate network.
- –VPN tunnel can be constructed all the way from the remote user to the corporate network

- The generic classification scheme has been used due to the blurring of the differences between traditional VPN types and also due to the fact that different providers have proposed a new type of VPN, namely, a network-based VPN



Security Requirements

- Confidentiality
- Integrity
- Authentication.
- Certification.
- Access Control
- Key Management.

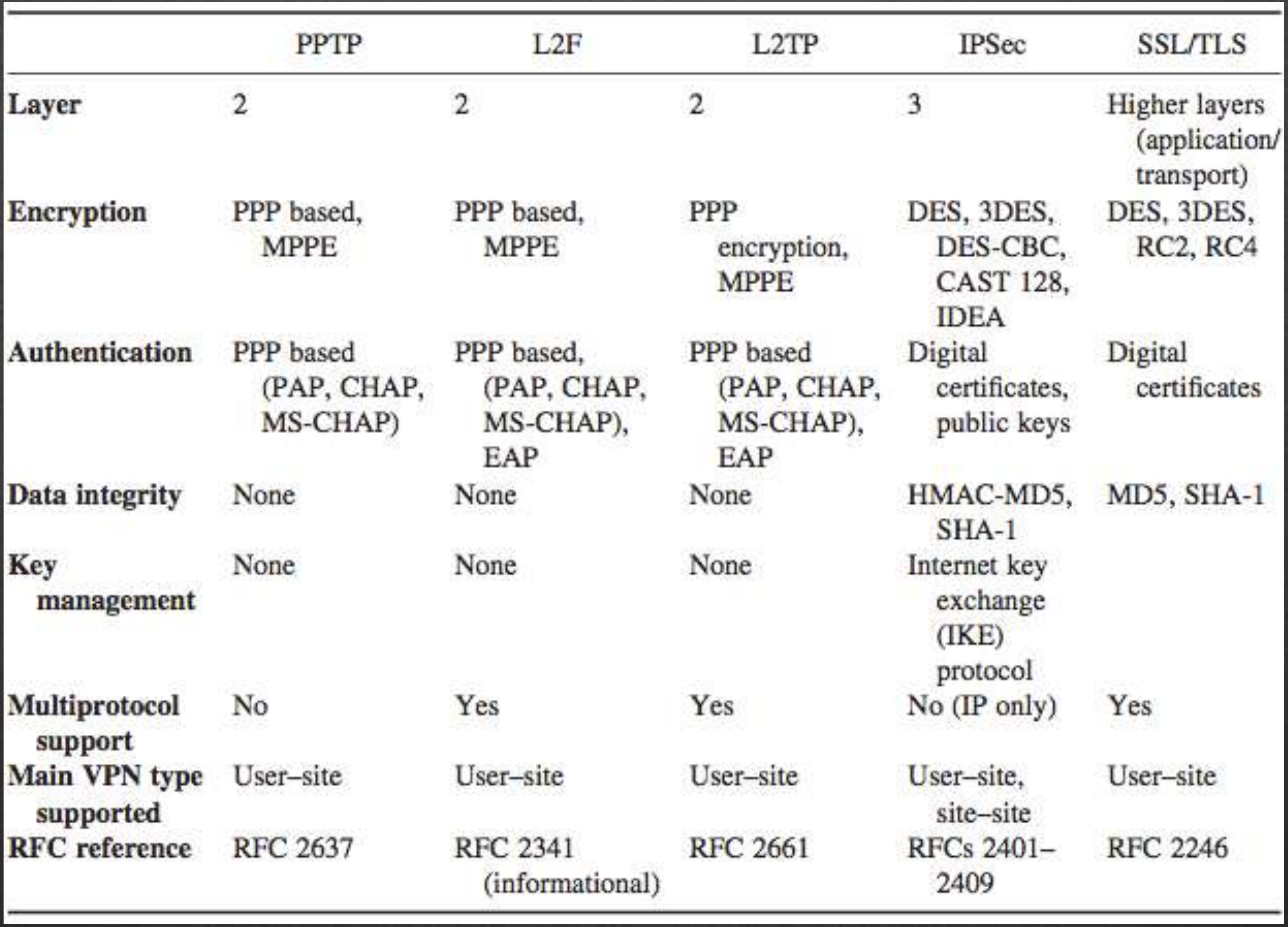
Tunneling Protocols

- PPTP (Point-to-Point Tunneling Protocol)
  - (RFC) 2637
  - Namely MS- PPP encryption (MPPE) and MS-CHAP have been proposed.
  - Encryption and authentication mechanisms provided by PPP,
    - » DES (data encryption standard) and 3-DES for encryption and
    - » PAP (Password Authentication Protocol)
    - » CHAP (Challenge Handshake Authentication Protocol) for authentication.

- L2F (Layer 2 Forwarding)
  - Cisco proposed a proprietary layer 2 tunneling protocol called L2F as a competitor for PPTP
  - It uses PPP for encryption and authentication but extends authentication to support TACACS+ (Terminal Access Controller Access Control System) and RADIUS (Remote Authentication Dial-in User Service) authentication by using EAP (Extensible Authentication Protocol).
- L2TP (Layer 2 Tunneling Protocol): RFC 2661
  - This layer 2 protocol includes all the features of PPTP and L2F
  - Provides authenticated and encrypted access from desktops to remote-access servers

- IPSec(IPSecurity)
  - IPSec is a set of open standards for a layer 3 tunneling protocol for VPNs
  - While PPTP, L2F, and L2TP are mainly applicable to user–site VPNs, IPSec can be targeted for both site–site and user–site VPNs
- SSL/TLS (Secure Sockets Layer/Transport Layer Security)
  - SSL is an application layer tunneling protocol that is supported by most Web browsers to secure HyperText Transfer Protocol (HTTP) documents.
  - SL/TLS provides server authentication by digital certificates and an optional server–client sub authentication
  - Encryption is by DES, 3DES, RC2 (Rivest Cipher 2), or RC4 (Rivest Cipher 4), and keyed hash MD-5 (Message Digest 5) and SHA-1 (secure hash algorithm) ensure message integrity

Summary



	PPTP	L2F	L2TP	IPSec	SSL/TLS
Layer	2	2	2	3	Higher layers (application/ transport)
Encryption	PPP based, MPPE	PPP based, MPPE	PPP encryption, MPPE	DES, 3DES, DES-CBC, CAST 128, IDEA	DES, 3DES, RC2, RC4
Authentication	PPP based (PAP, CHAP, MS-CHAP)	PPP based, (PAP, CHAP, MS-CHAP), EAP	PPP based (PAP, CHAP, MS-CHAP), EAP	Digital certificates, public keys	Digital certificates
Data integrity	None	None	None	HMAC-MD5, SHA-1	MD5, SHA-1
Key management	None	None	None	Internet key exchange (IKE) protocol	
Multiprotocol support	No	Yes	Yes	No (IP only)	Yes
Main VPN type supported	User–site	User–site	User–site	User–site, site–site	User–site
RFC reference	RFC 2637	RFC 2341 (informational)	RFC 2661	RFCs 2401–2409	RFC 2246

Try to:

- Configure VPN in Linux
- Configure VPN in Windows
- Compare and give your analysis