Encrypting Wireless Data with VPN Techniques

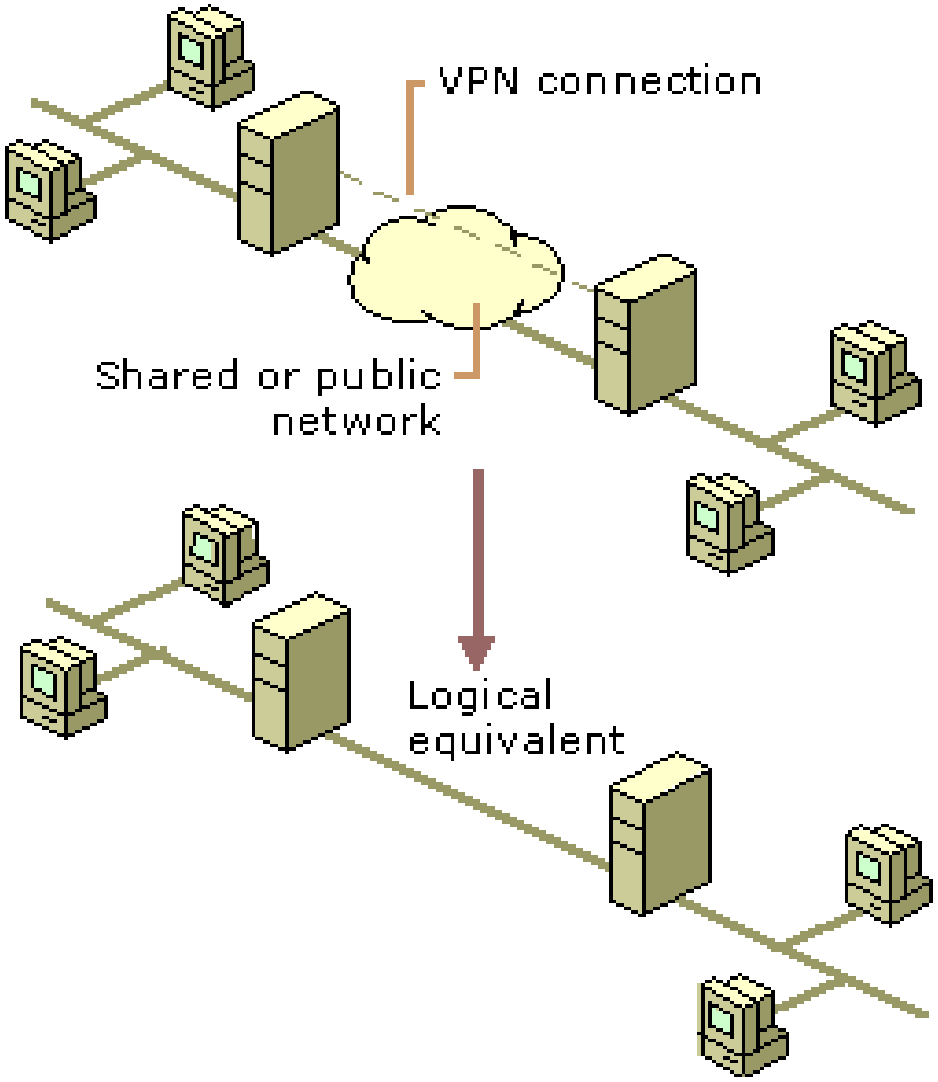
Topics

- Objectives
- VPN Overview
- Common VPN Protocols
- Conclusion

Objectives

- Recognize and Understand the common VPN Technologies.
- Compare the advantages and disadvantages of VPN technology and 802.1X/EAP types in 802.11 WLANs.

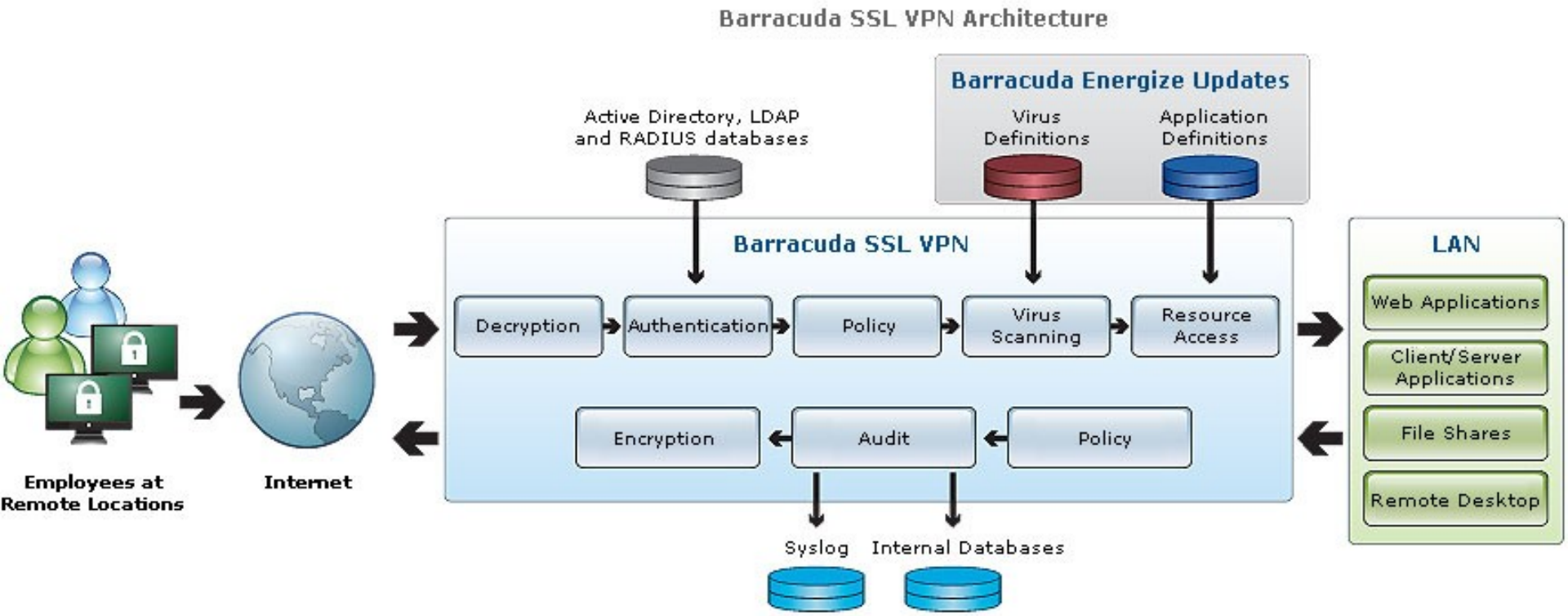
the logical equivalent of a VPN connection.



Virtual Private Network

- VPN technology provides several methods for one computer to securely communicate with another computer via a completely unsecured network.
- The components that make up a VPN consists of :
  - VPN-enabled routers and firewalls
  - VPN concentrators
  - Wireless routers and switches supporting direct VPN termination.
  - Enterprise Encryption Gateways
  - Enterprise Wireless Gateways
  - File Servers with operating system services or daemons supporting VPN terminations.

the logical equivalent of a VPN connection.



VPN Concentrator

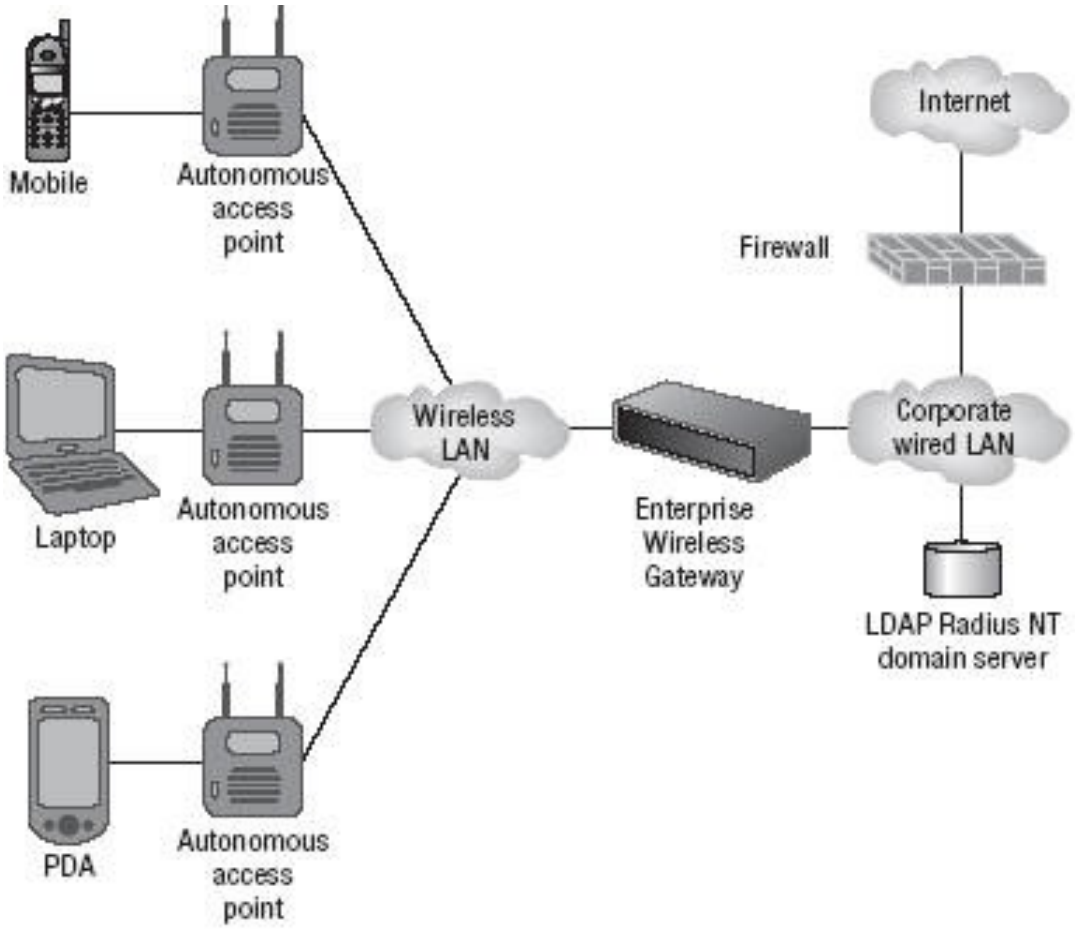


Cisco VPN Concentrator 3015 - VPN gateway

EEG
Enterprise Encryption Gateway



EWG
Enterprise Wireless Gateway



VPN Pros and Cons

- Advantages to both VPN and 802.11 security mechanisms:
  - Very secure encryption is available.
  - Well established standards are readily available from many vendors.
  - Authentication can be performed through a web browser, allowing almost any type of user access to the network.

Cont…

- The advantages of using VPNs in wireless environment include:
  - Many security administrators already understand VPN technology.
  - Most VPN servers work with established authentication methods like RADIUS.

Cont…

- Disadvantages of VPN technology in wireless environment include:
  - High encryption/decryption overhead.
  - More moving parts and more likely to break.
  - Clients and servers can be difficult to configure, deploy and maintain.
  - Expensive in almost any size network.
  - Advanced routing is difficult
  - Lack of interoperability between different vendors of VPN technology.
  - Lack of operating system support across multiple platforms.

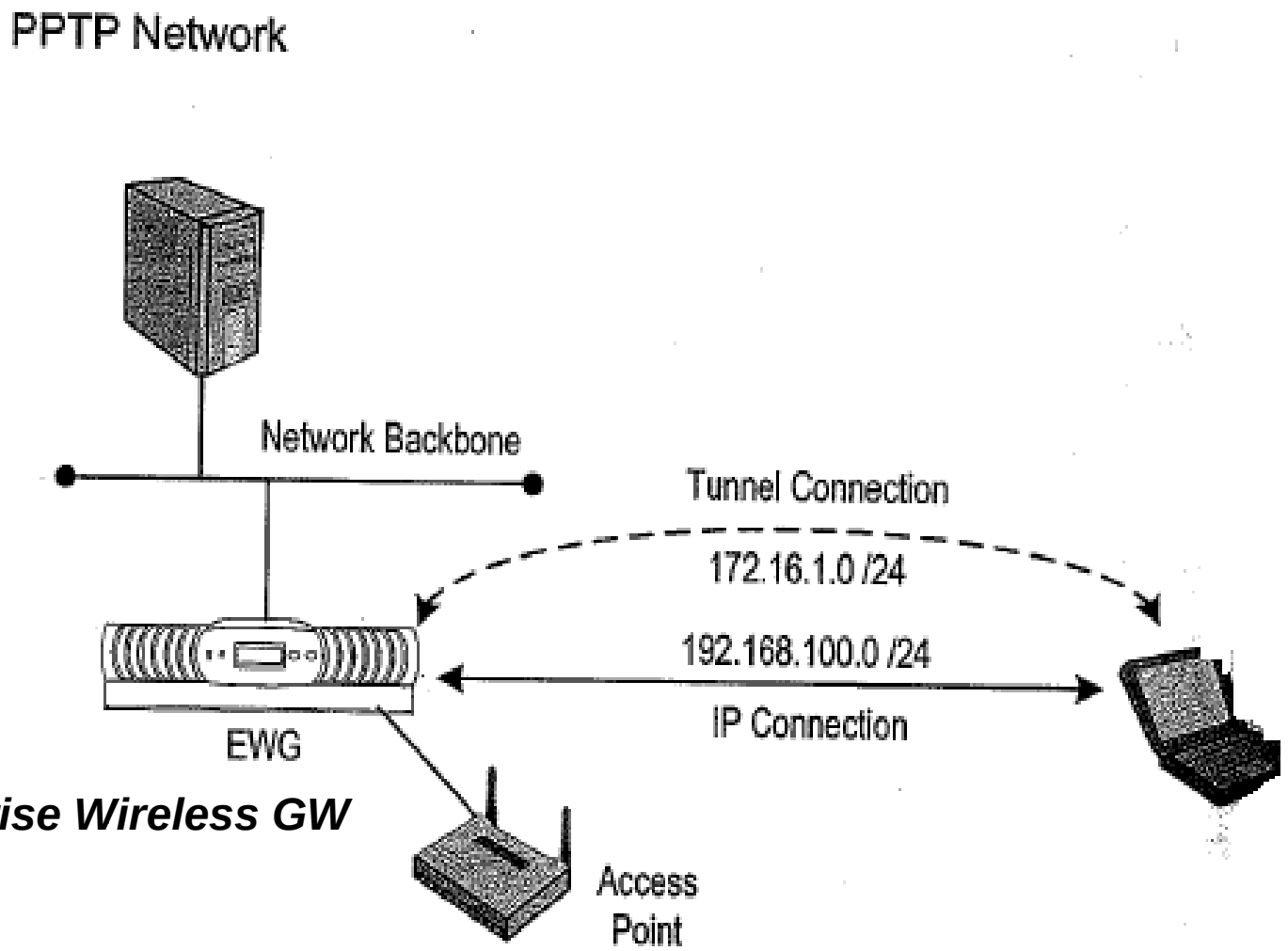
Common VPN Protocols

- There are many types of VPN protocols used in conjunction with wireless LAN such as
  - PPTP
  - L2TP
  - IPSec
  - SSL
  - SSH2

PPTP

- Point-to-Point-Tunneling Protocol (PPTP), developed by Microsoft and is based on Point-to-Point Protocol (PPP).
- It is commonly available client/server VPN technology that supports multiple encapsulated protocols, authentication and encryption.

PPTP Network



Enterprise Wireless GW

L2TP

- Layer 2 Tunneling Protocol (L2TP) is a VPN technology co-developed by Cisco and Microsoft by combining the best components of Cisco's Layer 2 Forwarding (L2F) and Microsoft's Point-to-Point Tunneling Protocol (PPTP).
- The two endpoints of an L2TP tunnel are:
  - **The LAC (L2TP Access Concentrator)**
  - **LNS (L2TP Network Server)**
- Allows multiple tunnels with multiple sessions inside every tunnel.
- Commonly used with IPSec -> L2TP/IPSec
- L2TP/IPSec connections use the Data Encryption Standard (DES) block cipher algorithm.

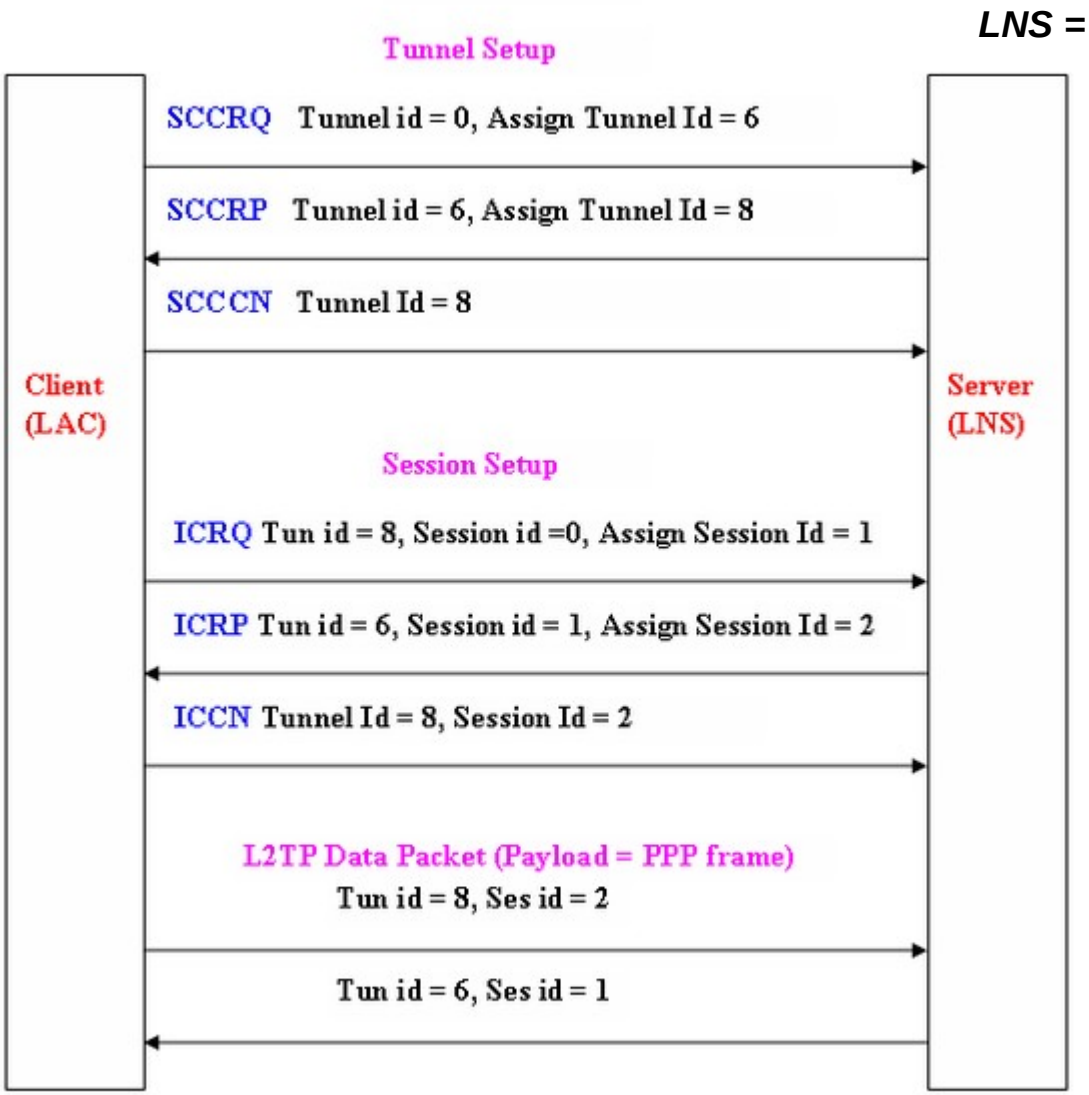
L2TP packet

An L2TP packet consists of :

Bits 0–15	Bits 16–31
Flags and Version Info	Length (opt)
Tunnel ID	Session ID
Ns (opt)	Nr (opt)
Offset Size (opt)	Offset Pad (opt).....
Payload data	

L2TP packet exchange

LAC = L2TP Access Concentrator
LNS = L2TP Network Server)



L2TP Control and Data Packets

IPSec

- IPsec (IP security) is a suite of protocols for securing Internet Protocol (IP) communications by authenticating and/or encrypting each IP packet in a data stream.
- IPsec also includes protocols for cryptographic key establishment.
- The two main protocols used in IPSec :
  - **Authentication Header:** It provides integrity and authentication and non-repudiation, if the appropriate choice of cryptographic algorithms is made.
  - **Encapsulating Security Payload:** It provides confidentiality, along with optional authentication and integrity protection.

How to set up IPSec/VPN windows (vista/7)

- http://rapidvpn.com/setup_l2tp_vpn_windows_vista

SSL/TLS

- Security Socket Layer/ Transport Layer Security (SSL/TLS) VPN technology is developed by Netscape.
- Advantages of SSL VPN include:
  - An SSL VPN is clientless.
  - Users have access from anywhere there is a connection and a supported browser as opposed to a computer with custom VPN software installed and configured.
  - Since SSL is an application layer protocol, it is possible to more easily apply granular access to various user roles.

Cont…

- Disadvantages of an SSL VPN include:
  - Not well suited for point-to-point encrypted links.
  - Only usable for applications that interact with a web browser.

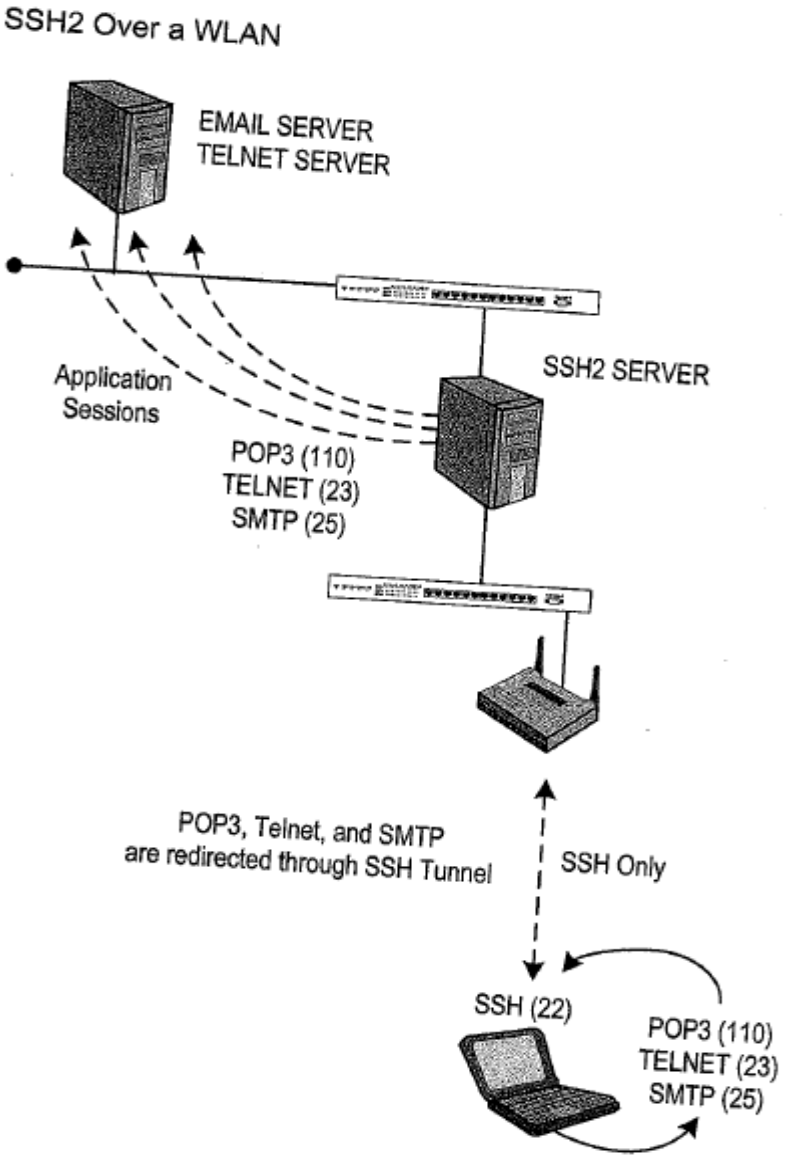
SSH2

- SSH2 (Secure Shell v2) is a protocol implemented in an application that provides an authenticated, cryptographically secure TCP/IP tunnel between two computers.
- SSH2 has the following features:
  - Public and private key authentication or the client's username/password.
  - Public and private key data signing
  - Private key passphrase association
  - Data encryption with multiple cipher support
  - Encryption key rotation
  - Data integrity using Message Authentication Code algorithms
  - Data compression
  - Troubleshooting log messages

Cont…

- SSH2 provides three main capabilities:
  - Secure command shell
  - Secure file transfer
  - Port forwarding

Cont…


SSH2 Over a WLAN
EMAIL SERVER
TELNET SERVER
Application
Sessions
SSH2 SERVER
POP3 (110)
TELNET (23)
SMTP (25)
POP3, Telnet, and SMTP
are redirected through SSH Tunnel
SSH Only
SSH (22)
POP3 (110)
TELNET (23)
SMTP (25)

Conclusion

- VPNs operate at OSI layer 3 through 7 in contrast to 802.11security mechanisms that operate at layer 2.
- VPNs over wireless is not always the best choice because of the limitations of VPNs can place on wireless mobility and scalability.