

# Wireless Security

Christopher Rees

<https://www.linkedin.com/in/cdreer>

@cdreer



**pluralsight**   
hardcore dev and IT training

# Wireless Security Objectives

## Security Issues Related to **Wireless Networking**

- ❑ WPA
- ❑ WPA2
- ❑ WEP
- ❑ EAP
- ❑ PEAP
- ❑ LEAP
- ❑ MAC Filter
- ❑ Disable SSID Broadcast
- ❑ TKIP
- ❑ CCMP
- ❑ Antenna Placement
- ❑ Power Level Controls
- ❑ Captive Portals
- ❑ Antenna Types
- ❑ Site Surveys
- ❑ VPN (over open wireless)

# IEEE 802.11x Wireless Protocols

- Wireless communication over 802.11 standards operate over 2.4 GHz and 5 GHz radio frequencies

Standard	Speed(s)	Frequencies
802.11	1 Mbps or 2 Mbps	2.4GHz
802.11a	54 Mbps	5 GHz
802.11b	11 Mbps	2.4GHz
802.11g	54 Mbps	2.4GHz
802.11n	Up to 600 Mbps	2.4GHz or 5GHz

- *802.11i is often referred to WPA2 and provides for additional security enhancements focused on authentication*

# Wireless Definitions

- **Wired Equivalency Protocol (WEP)**
  - Originally designed to provide security equal to a wired network
  - Vulnerabilities emerged and has since been deprecated
- **Wi-Fi Protected Access (WPA/WPA2)**
  - WPA was based on WEP and used as a stop gap
  - WPA2 fully implements to the full 802.11i protocol and provides additional security enhancements
- **Wireless Application Protocol (WAP)**
  - Used to provide mobile devices with internet connectivity
  - Suite of protocols similar to TCP/IP
  - Uses Wireless Transport Layer Security (WTLS)
    - Authentication, encryption, and data integrity
    - Connectionless protocol similar to TLS

# WEP/WPA/WPA2

Standard	Method	Security	Notes
WEP	RC4 Stream	24-bit encryption	IV attack/Packet injection can crack WEP in several seconds
WPA	TKIP	128-bit encryption	TKIP has been cracked as well
WPA2	AES-CCMP	128-bit encryption	48-bit IV makes it much more secure

## ■ WEP Weakness

- Initialization Vector (IV) is only 24 bits long
  - Sent in clear text
  - IV is static and is reused
  - IV is part of the RC4 encryption key
- 
- WEP should be **avoided** unless backward compatibility with older devices is needed

# WPA and WPA2

- **WPA partially implements the 802.11i standard**

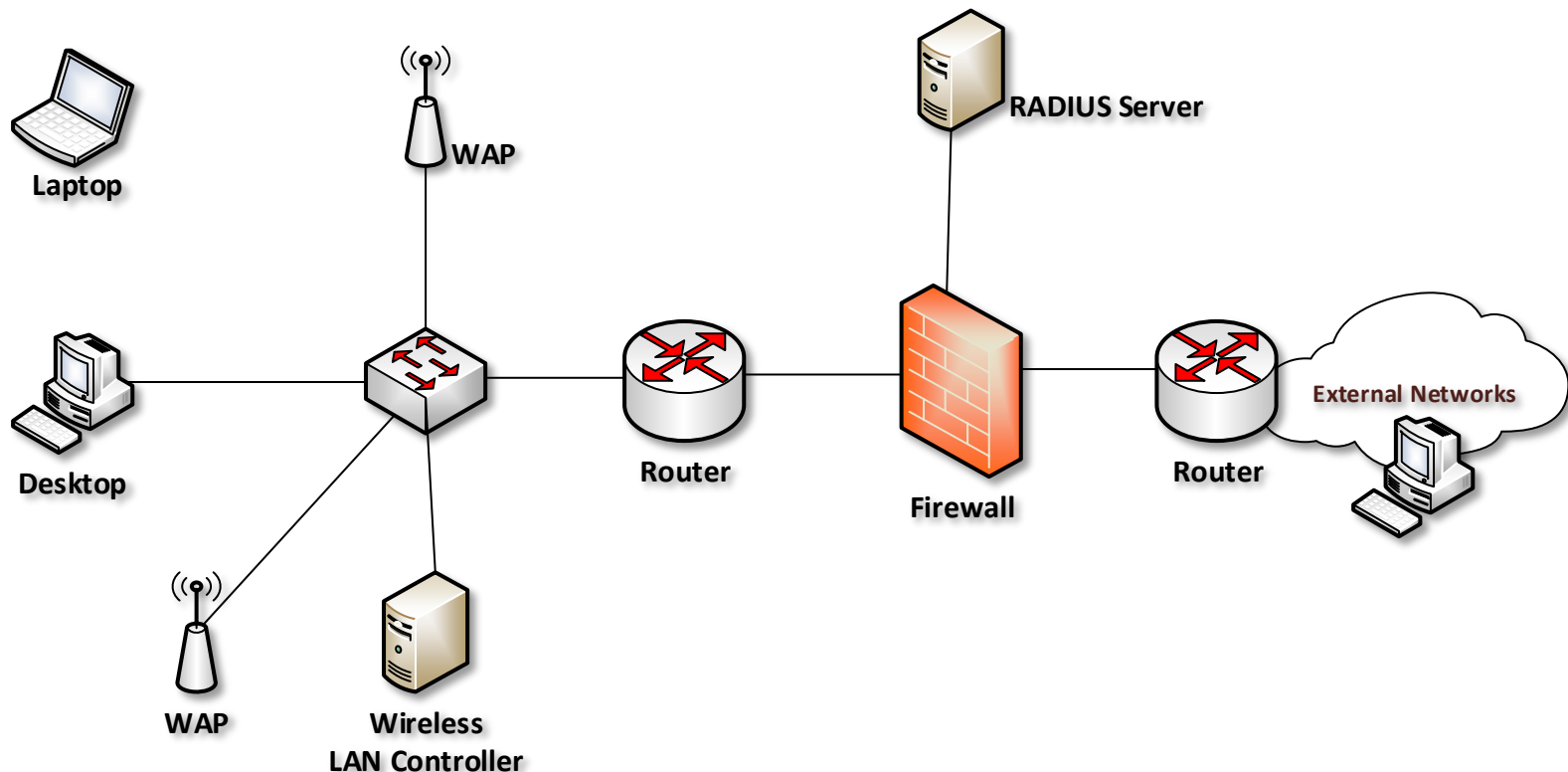
- Uses **TKIP** (Temporal Key Integrity Protocol)
- 128-bit wrapper around the WEP encryption
  - Second key based on MAC address of sender and serial # of the packet
  - Mixes this key with the Initialization Vector to create a per packet key
- RC4 encryption still used
- Backward compatible with WEP

- **WPA2 fully implements the 802.11i standard**

- Uses **CCMP** for enhanced security (CC-MAC Protocol)
  - Counter Mode Cipher Block Chaining Message Authentication Code Protocol
- 128-bit AES encryption used
- Not backward compatible with WEP

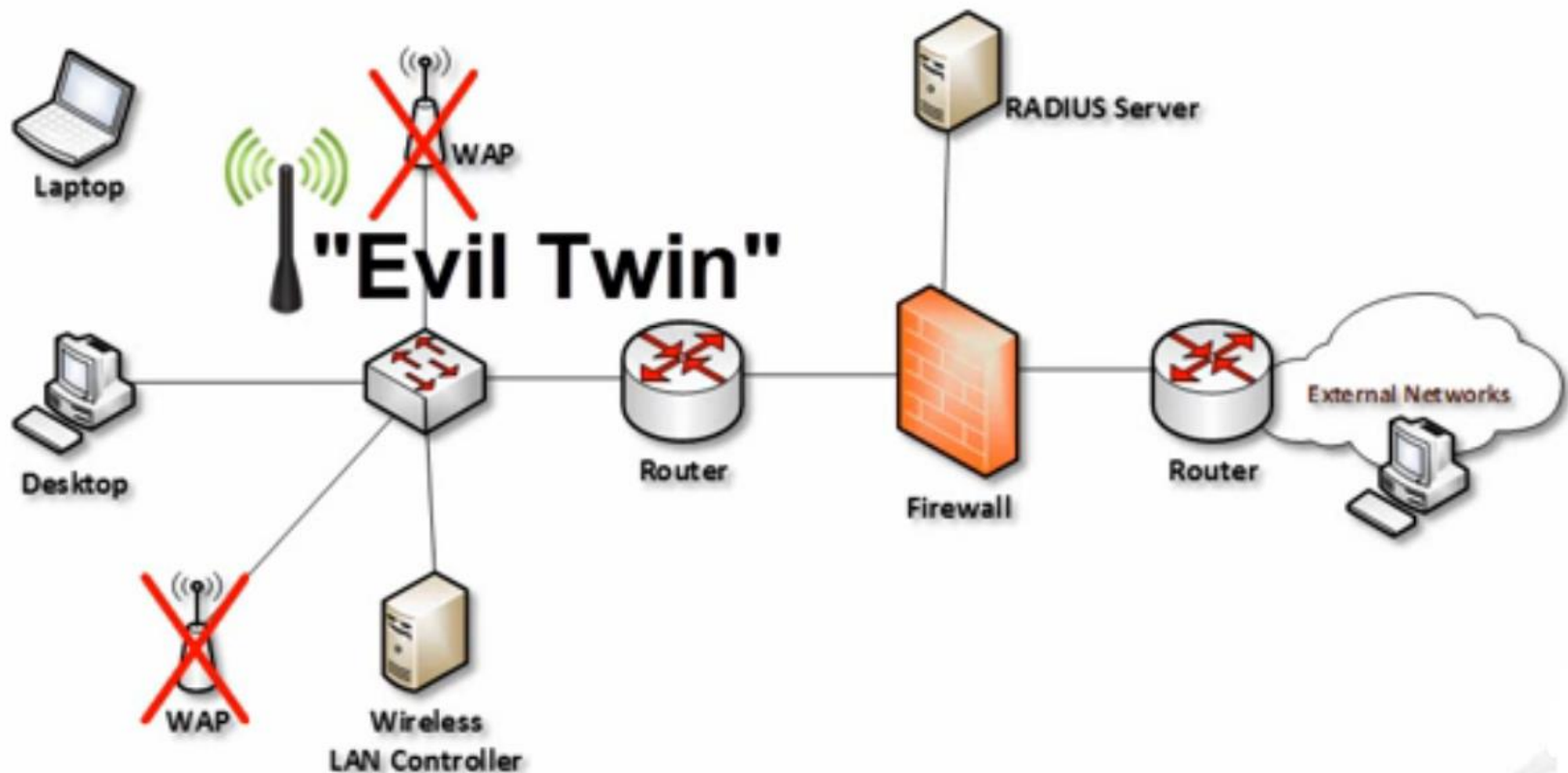
# Wireless Security Examples

- WPA/WPA2 can use **Pre-Shared Key (PSK)** or **Enterprise Authentication**
  - PSK is fine for home or SOHO networks
  - Enterprise uses RADIUS Server and Digital Certificates



# Wireless Security Examples

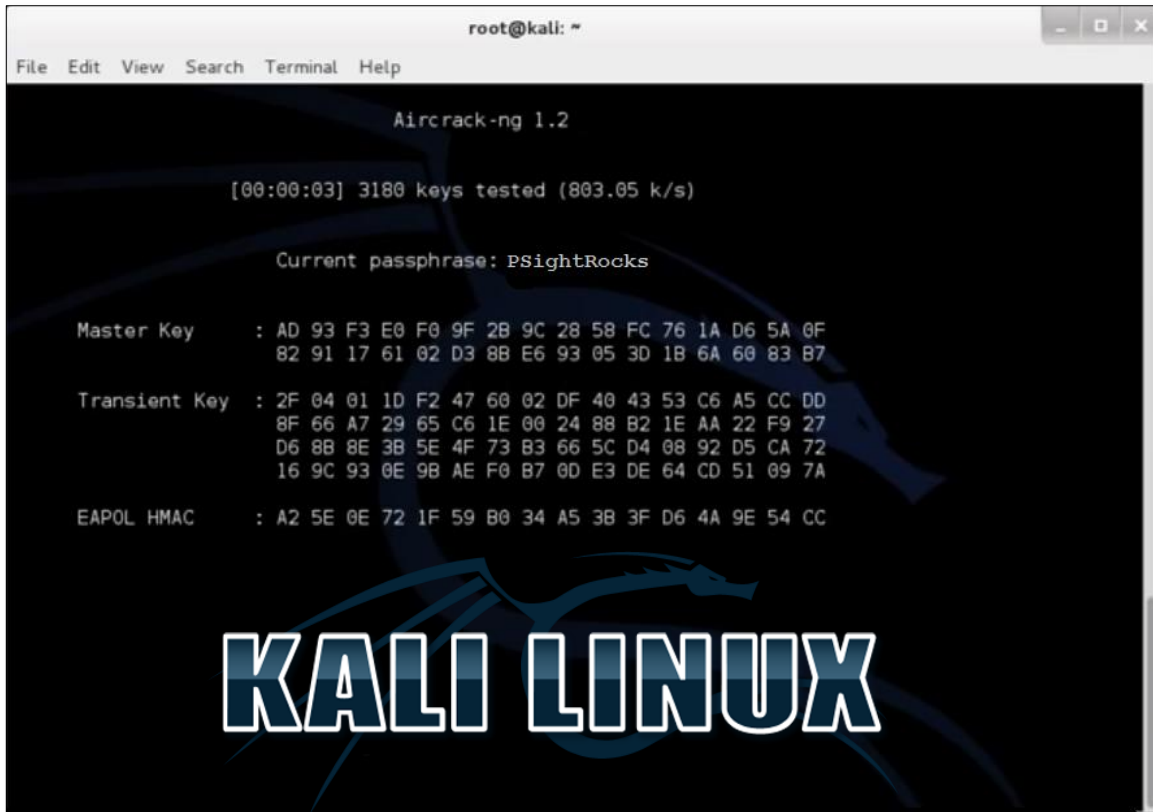
- WPA/WPA2 can use **Pre-Shared Key (PSK)** or **Enterprise Authentication**
  - PSK is fine for home or SOHO networks
  - Enterprise uses RADIUS Server and Digital Certificates





# Wireless Security

- Many off the shelf **Penetration Testing (PenTest)** tools can quickly compromise insecure wireless protocols
  - WEP and even WPA and WPA2!



```
root@kali: ~  
File Edit View Search Terminal Help  
Aircrack-ng 1.2  
[00:00:03] 3180 keys tested (803.05 k/s)  
Current passphrase: PSightRocks  
Master Key      : AD 93 F3 E0 F0 9F 2B 9C 28 58 FC 76 1A D6 5A 0F  
                  82 91 17 61 02 D3 8B E6 93 05 3D 1B 6A 60 83 B7  
Transient Key   : 2F 04 01 1D F2 47 60 02 DF 40 43 53 C6 A5 CC DD  
                  8F 66 A7 29 65 C6 1E 00 24 88 B2 1E AA 22 F9 27  
                  D6 8B 8E 3B 5E 4F 73 B3 66 5C D4 08 92 D5 CA 72  
                  16 9C 93 0E 9B AE F0 B7 0D E3 DE 64 CD 51 09 7A  
EAPOL HMAC     : A2 5E 0E 72 1F 59 B0 34 A5 3B 3F D6 4A 9E 54 CC  
KALI LINUX
```

- Locate wireless networks
- Capture packets
- De-authenticate nodes connected to wireless access point
- Capture 4-way handshake as they reconnect
- Brute force / dictionary attack / hash attack to discover the password
- Use other tools to crack the WPS PIN to obtain the WPA/WPA2 password

# EAP, PEAP and LEAP

- Extensible Authentication Protocol
- A set of authentication frameworks for wireless networks
- 5 different types of EAP adopted by WPA/WPA2 standard
  - EAP-TLS
  - EAP-PSK
  - EAP-MD5
  - LEAP
  - PEAP

# LEAP and PEAP

- **LEAP (Lightweight Extensible Authentication Protocol)**

- Proprietary protocol developed by Cisco as a stop gap to WEP and lacked Windows support
- Easy to configure / no digital certificates
- Clear text transmissions
- Since deprecated

- **PEAP (Protected Extensible Authentication Protocol)**

- Joint development effort by Cisco, RSA and Microsoft
- Windows support
- Digital certificate used on the authentication server
- Establishes encrypted channel between client and server via TLS tunnel

# Wi-Fi Security Best Practices

- **Disable SSID Broadcast**

- Service Set Identifier (Wi-Fi Network Name)
- *Doesn't really provide security, SSID can still be sniffed*



~~Security  
by  
Obscurity~~

# Wi-Fi Security Best Practices

- **Disable SSID Broadcast**

- Service Set Identifier (Wi-Fi Network Name)
- *Doesn't really provide security, SSID can still be sniffed*

- **Use MAC Filtering**

- Pre-select what MAC addresses can connect to the Wi-Fi network
- *Vulnerable to MAC spoofing*

- **Common Sense Administration**

- Always change default admin username and password
- Use strongest encryption/authentication available
- Keep access points up to date (patches and firmware)



# Wi-Fi Security Best Practices

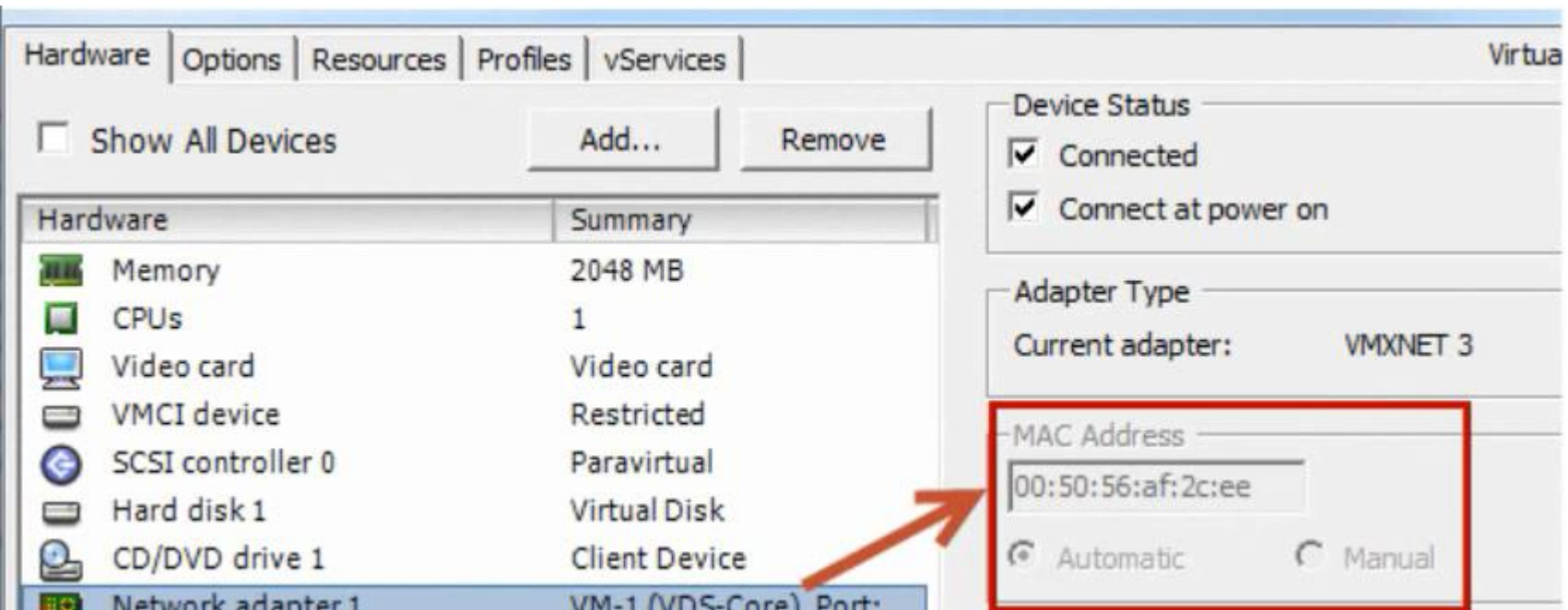
- **Disable SSID Broadcast**

- Service Set Identifier (Wi-Fi Network Name)
- *Doesn't really provide security, SSID can still be sniffed*



- **Use MAC Filtering**

- Pre-select what MAC addresses can connect to the Wi-Fi network
- *Vulnerable to MAC spoofing*



# Antenna Placement

- **Antenna placement is critical for proper coverage**
  - Should be placed near the center of the area to be covered
  - Antennas can be **internal** or **external**



# Antenna Placement

- **Antennas can be omnidirectional or unidirectional**
  - Omnidirectional provides 360-degree coverage
  - Directional antennas focus the signal in one direction (usually over longer distances)



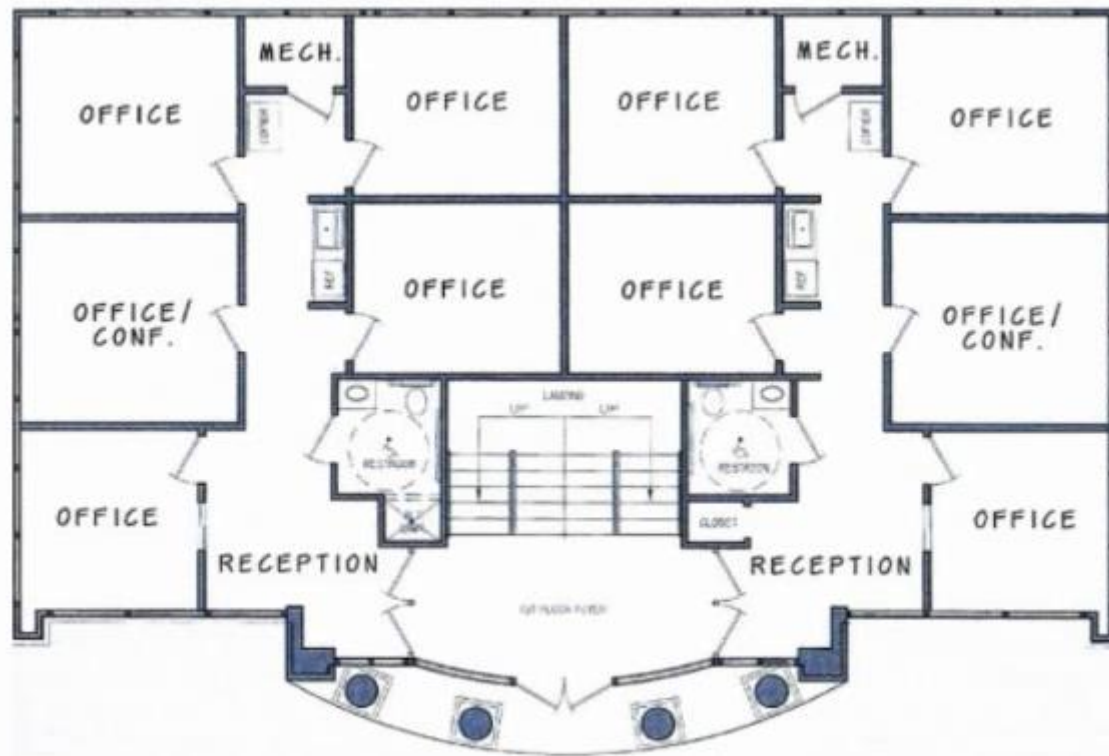


# Power Level Controls

- **Antenna Signal Strength**
  - Antennas are rated in terms of gain value or dBi numbers
  - A wireless antenna with a 10 dBi would be 10x stronger than 0 dBi

# Power Level Controls

- **Antenna Signal Strength**
  - Antennas are rated in terms of gain value or dBi numbers
  - A wireless antenna with a 10 dBi would be 10x stronger than 0 dBi



# Power Level Controls

- **Antenna Signal Strength**
  - Antennas are rated in terms of gain value or dBi numbers
  - A wireless antenna with a 10 dBi would be 10x stronger than 0 dBi
- **Some wireless routers provide control**
  - Turn power levels up or down depending on environment
  - Combine with Site Survey to identify optimal placement(s)

# Power Level Controls

- **Antenna Signal Strength**
  - Antennas are rated in terms of gain value or dBi numbers
  - A wireless antenna with a 10 dBi would be 10x stronger than 0 dBi
- **Some wireless routers provide control**
  - Turn power levels up or down depending on environment
  - Combine with Site Survey to identify optimal placement(s)



# Power Level Controls

- **Antenna Signal Strength**
  - Antennas are rated in terms of gain value or dBi numbers
  - A wireless antenna with a 10 dBi would be 10x stronger than 0 dBi
- **Some wireless routers provide control**
  - Turn power levels up or down depending on environment
  - Combine with Site Survey to identify optimal placement(s)



# Site Survey

- **Assessment of the area for signal strength, SSID broadcast, encryption, etc.**
- **Can be good or bad**
  - Good
    - Determines optimal AP placement(s)
      - Minimizes interference, provides for optimal signal throughout building
  - Bad
    - Can be used by hackers to determine equipment, protocols, security, etc
    - Sometimes referred to as **War Driving and War Chalking**

# War Chalking



# War Chalking

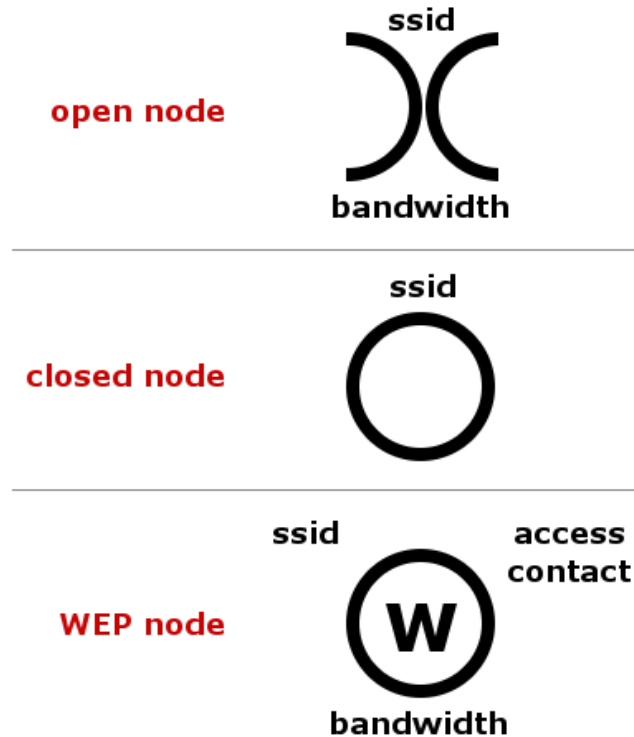
- **Symbols drawn on sidewalks, sides of buildings, etc**
  - Lets hackers know what type(s) of networks are present





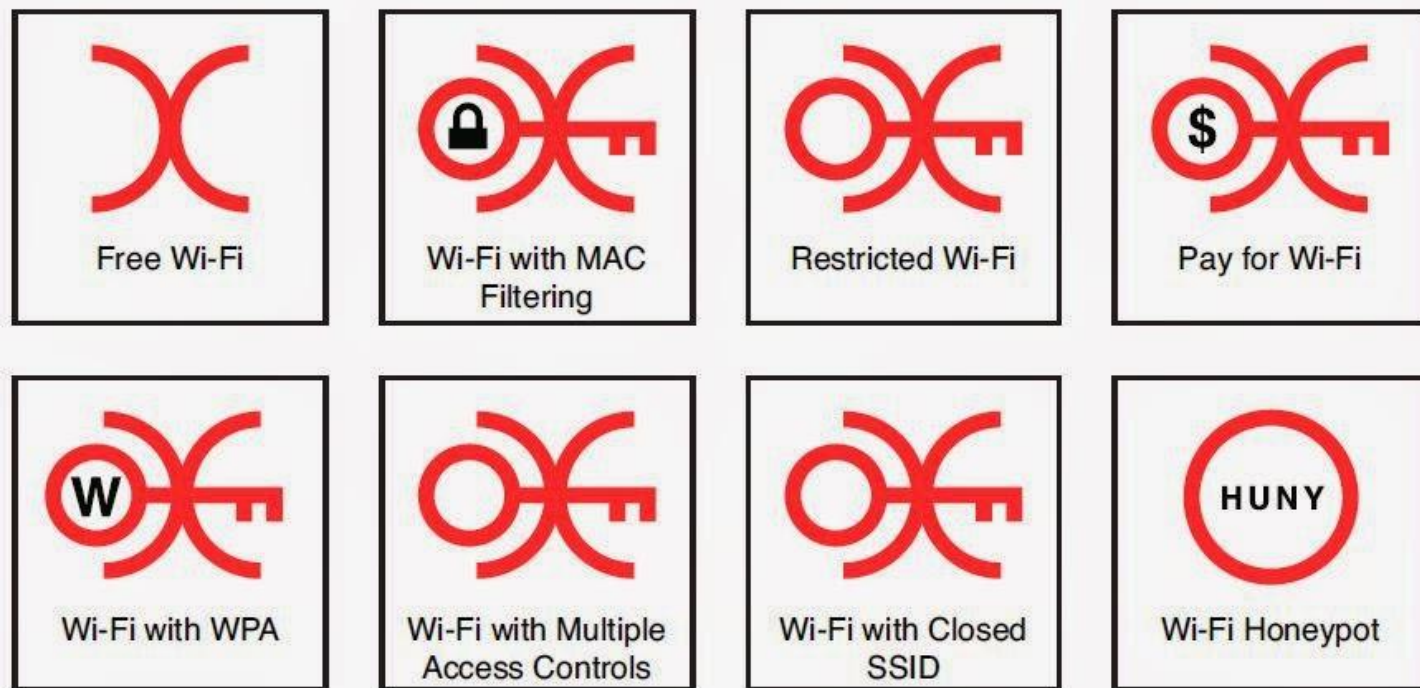
# War Chalking

- Symbols drawn on sidewalks, sides of buildings, etc
  - Lets hackers know what type(s) of networks are present



# War Chalking

- Symbols drawn on sidewalks, sides of buildings, etc
  - Lets hackers know what type(s) of networks are present



# **VPN (Over Open Wireless)**

- **VPN is well suited for use over an open wireless network**
  - Secure tunnel is established
  - Allows for secure browsing, connection to remote office, etc
- **VPN can be established at the Data Link or Network Layer**
  - IPSec or SSL

# Captive Portal

**PUBLIC WI-FI**

[Register](#)

[Help](#)

[My Account](#)



# Hello

[Click here](#) to register for free Internet access...  
If you have an account, login below.

Username

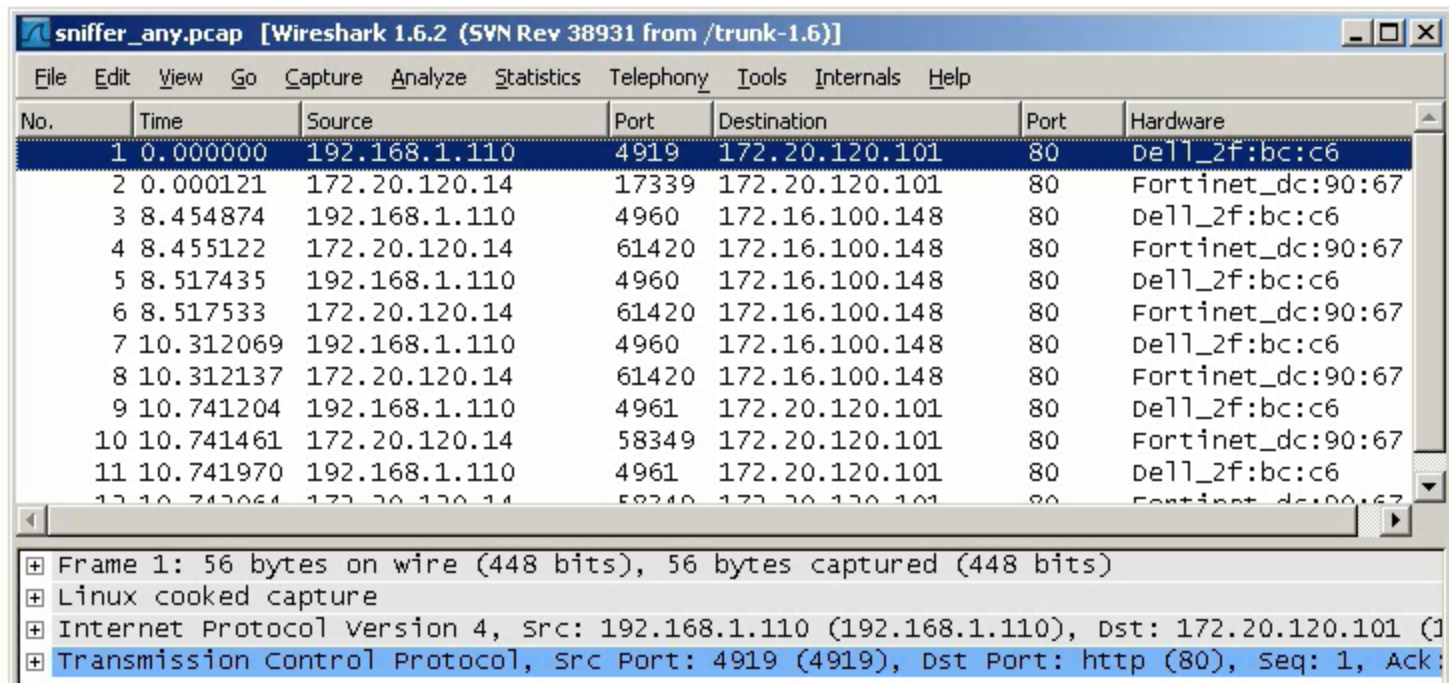
Password

Login

[Forgot Password?](#)

# Captive Portal

- **Authentication or acceptance page typically found in open and public networks**
  - Requires the user to enter credentials, agree to acceptable use policies, make payment, etc., before granting access
  - Vulnerable to packet sniffing
    - Once a user is authenticated a hacker could sniff the packets and determine IP address and MAC address then spoof them to gain access



The image shows a Wireshark 1.6.2 window titled "sniffer\_any.pcap [Wireshark 1.6.2 (SVN Rev 38931 from /trunk-1.6)]". The main pane displays a list of 11 captured packets. The first packet is selected, and the bottom pane shows its details.

No.	Time	Source	Port	Destination	Port	Hardware
1	0.000000	192.168.1.110	4919	172.20.120.101	80	Dell_2f:bc:c6
2	0.000121	172.20.120.14	17339	172.20.120.101	80	Fortinet_dc:90:67
3	8.454874	192.168.1.110	4960	172.16.100.148	80	Dell_2f:bc:c6
4	8.455122	172.20.120.14	61420	172.16.100.148	80	Fortinet_dc:90:67
5	8.517435	192.168.1.110	4960	172.16.100.148	80	Dell_2f:bc:c6
6	8.517533	172.20.120.14	61420	172.16.100.148	80	Fortinet_dc:90:67
7	10.312069	192.168.1.110	4960	172.16.100.148	80	Dell_2f:bc:c6
8	10.312137	172.20.120.14	61420	172.16.100.148	80	Fortinet_dc:90:67
9	10.741204	192.168.1.110	4961	172.20.120.101	80	Dell_2f:bc:c6
10	10.741461	172.20.120.14	58349	172.20.120.101	80	Fortinet_dc:90:67
11	10.741970	192.168.1.110	4961	172.20.120.101	80	Dell_2f:bc:c6

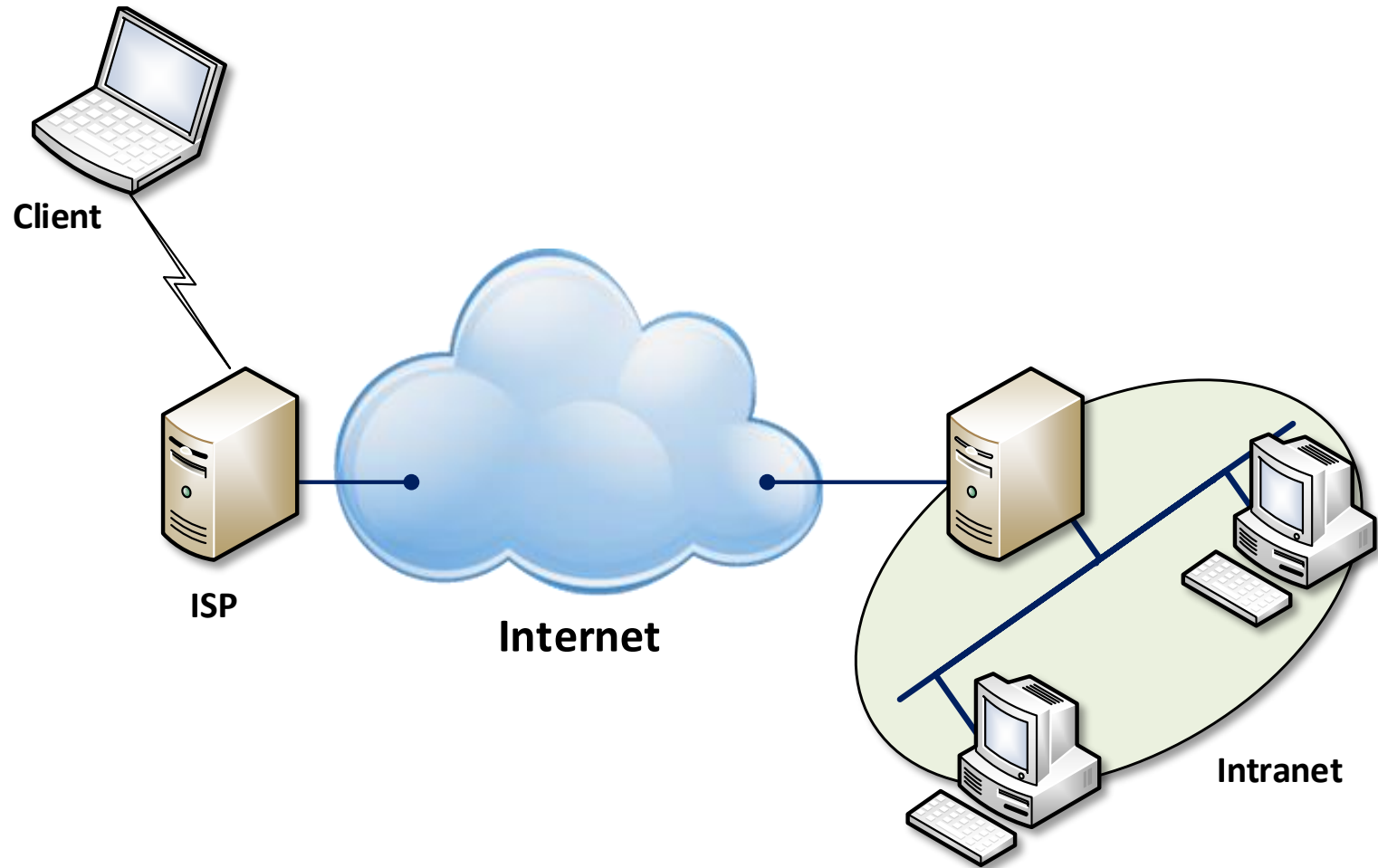
  

Frame 1: 56 bytes on wire (448 bits), 56 bytes captured (448 bits)	
Linux cooked capture	
Internet Protocol Version 4, Src: 192.168.1.110 (192.168.1.110), Dst: 172.20.120.101 (172.20.120.101)	
Transmission Control Protocol, Src Port: 4919 (4919), Dst Port: http (80), Seq: 1, Ack:	

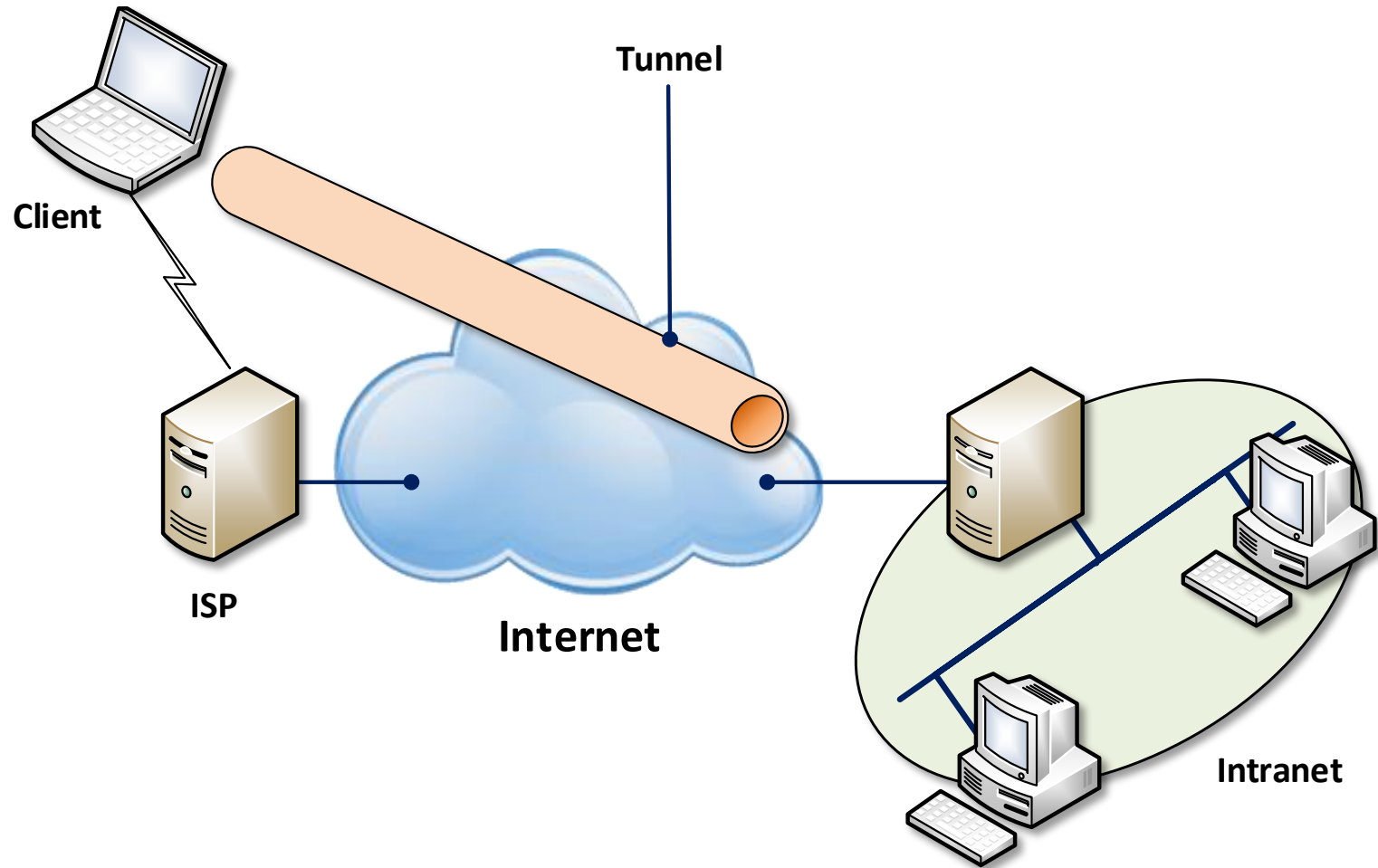
# Captive Portal

- **Authentication or acceptance page typically found in open and public networks**
  - Requires the user to enter credentials, agree to acceptable use policies, make payment, etc., before granting access
  - Vulnerable to packet sniffing
    - Once a user is authenticated a hacker could sniff the packets and determine IP address and MAC address then spoof them to gain access
- **Fake Captive Portal could be displayed to capture user credentials**

# VPN (Over Open Wireless)

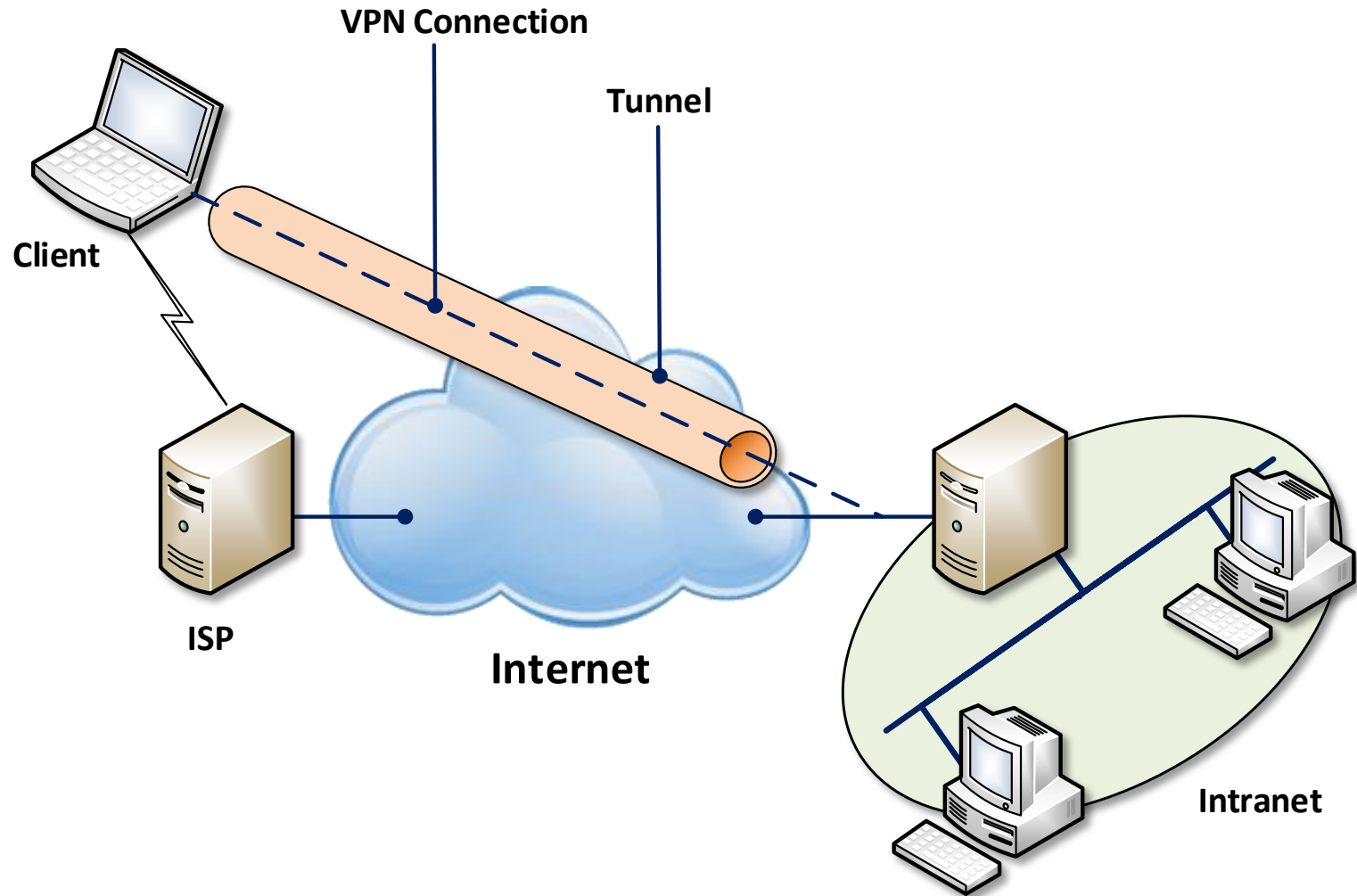


# VPN (Over Open Wireless)





# VPN (Over Open Wireless)



# Wireless Security Objectives

## Security Issues Related to **Wireless Networking**

- ❑ WPA
- ❑ WPA2
- ❑ WEP
- ❑ EAP
- ❑ PEAP
- ❑ LEAP
- ❑ MAC Filter
- ❑ Disable SSID Broadcast
- ❑ TKIP
- ❑ CCMP
- ❑ Antenna Placement
- ❑ Antenna Types
- ❑ Power Level Controls
- ❑ Site Surveys
- ❑ Captive Portals
- ❑ VPN (over open wireless)