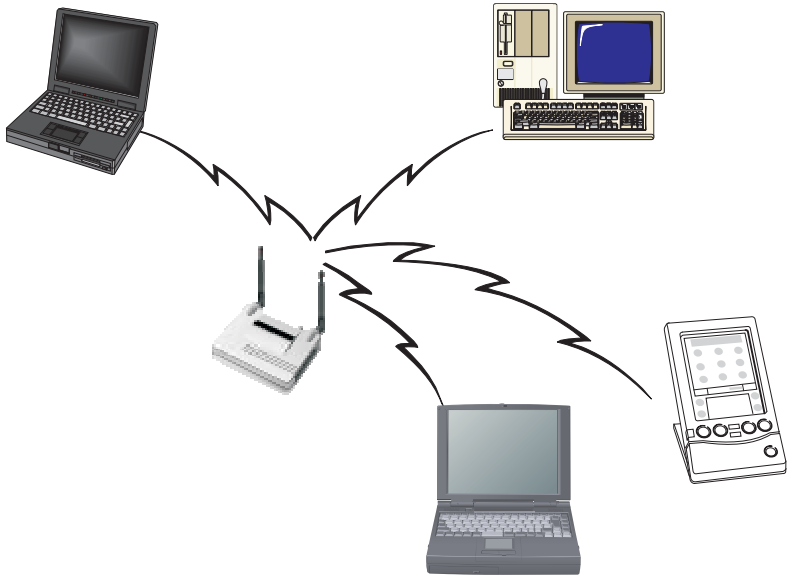
Wireless Network Security Challenges

SHARE Summer 2010 Seattle - Session 3126

Laura Knapp IBM Security Consultant laura@lauraknapp.com

Wireless is NOT Secure

Any questions?



Thank you, have a nice day!

Agenda

Introduction

SSID

MAC ID

WEP

802.1x

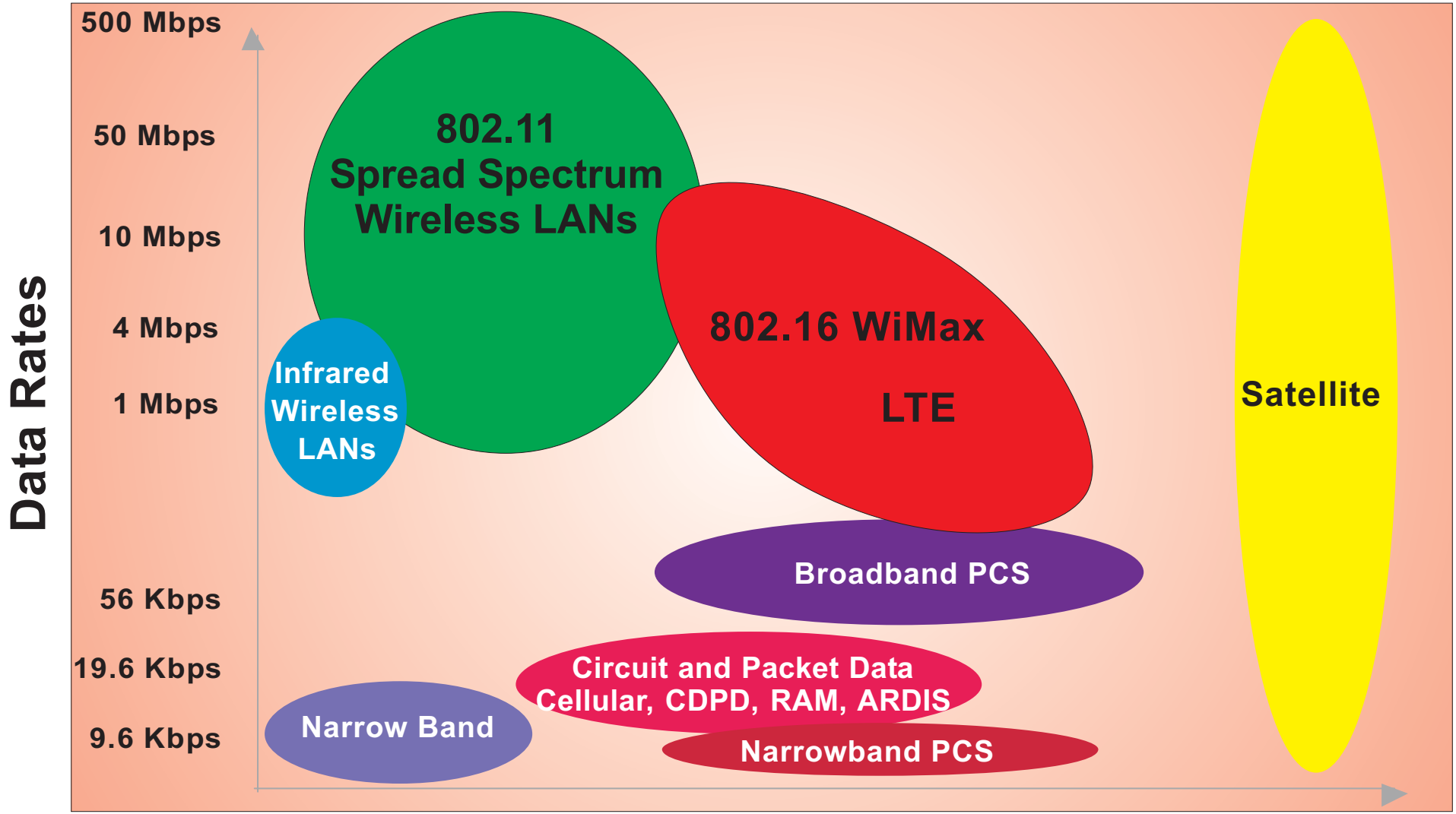
WPA

VPN

VLAN

Summary

Wireless Technologies



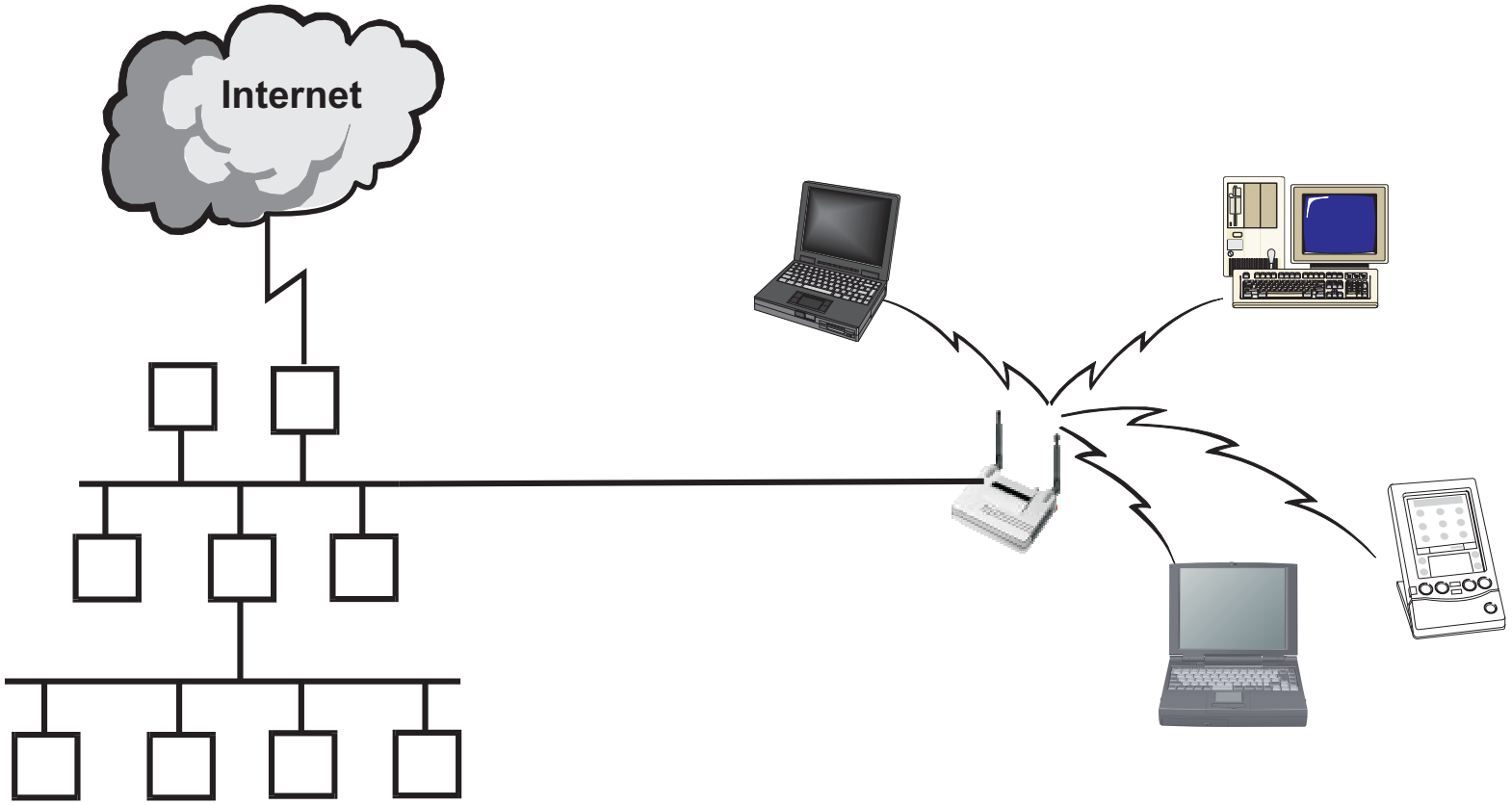
Wireless LAN Technologies

802.11b	802.11a	802.11g	802.11n ~~2007~~ 12/2009
2.4 GHz (3 non-overlap)	5 GHz (23 non-overlap)	2.4 GHz (3 non-overlap)	5 + 2.4 Ghz
Worldwide	FCC/Japan	Worldwide	Worldwide Versions
DSSS	OFDM	OFDM	MIMO OFDM
11 Mbps	54 Mbps	54 Mbps	500 Mbps?

The Laws of Radio Dynamics:

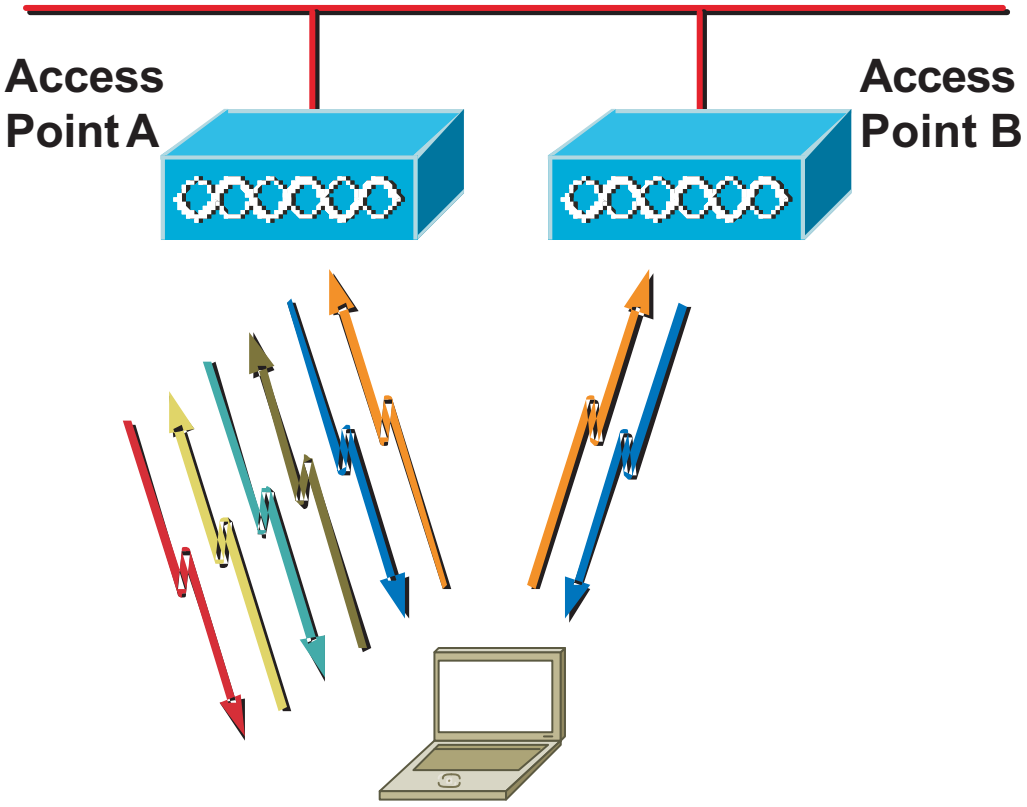
Higher data rates = shorter transmission range
Higher power output = increased range, but lower battery life
Higher frequency radios = higher data rates, shorter ranges

Wireless LAN Topology



All the devices on access point (AP) share bandwidth
Remember the performance issues of shared hubs
Switches provide interconnection (and management)
Protocols and applications work seamlessly

Association Process



Initial Connection to an Access Point

Steps to Association:

- Client sends probe
- AP sends Probe Response
- Client evaluates AP response, selects best AP
- Client sends authentication request to selected AP (A)
- AP A confirms authentication and registers client
- Client sends association request to selected AP (A)
- AP A confirms association and registers client

Primary Security Protocols

SSID - Service Set ID

MAC ID - Media Access Control ID

WEP - Wired Equivalent Privacy

802.1x - IEEE 802.1x standard

WPA - Wi-Fi Protected Access

VPNs - Virtual Private Networks

VLANs - Virtual Local Area Networks

Other protocols exist at higher levels, but we won't discuss them here Look into WSA (WAP Security Protocol) and WTLS (Wireless Transport Layer Security)

Agenda

Introduction

SSID

MAC ID

WEP

802.1x

WPA

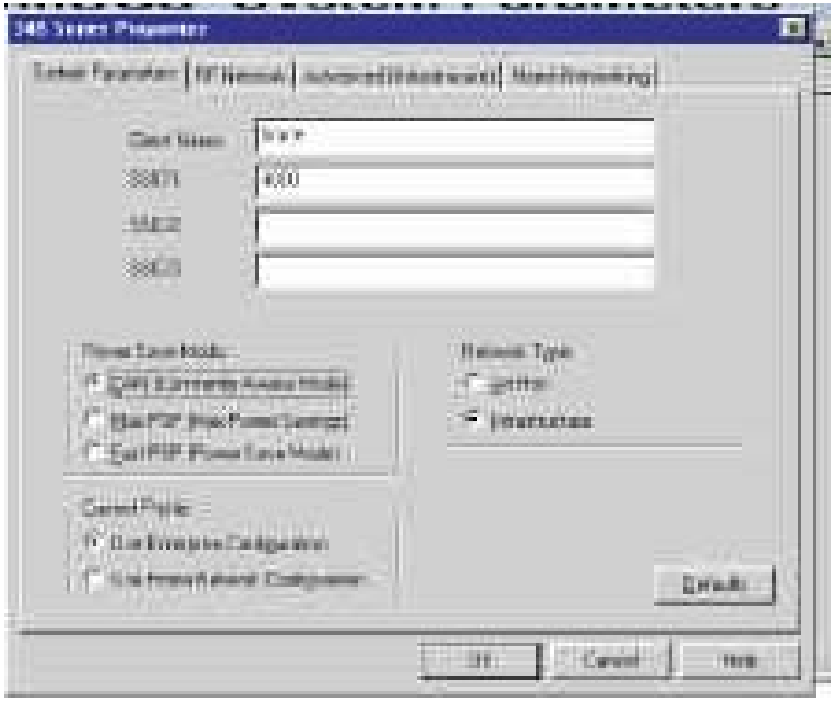
VPN

VLAN

Summary

SSID - Service Set ID

SSID is the network name for a wireless network



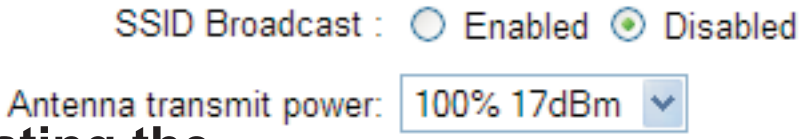
WLAN products ship with default names

- **Cisco = tsunami**
- **D-link = default**
- **Netgear = Netgear**

Default is to broadcast SSID -- Turn off

Can be required to specifically request the access point by name (SSID acts as a password)

The more the SSID is known the more likely that it will be misused.....however....in a large corporation you want everyone to know it



Changing the SSID requires communicating the change to all the users

Agenda

Introduction

SSID

MAC ID

WEP

802.1x

WPA

VPN

VLAN

Summary

MAC ID

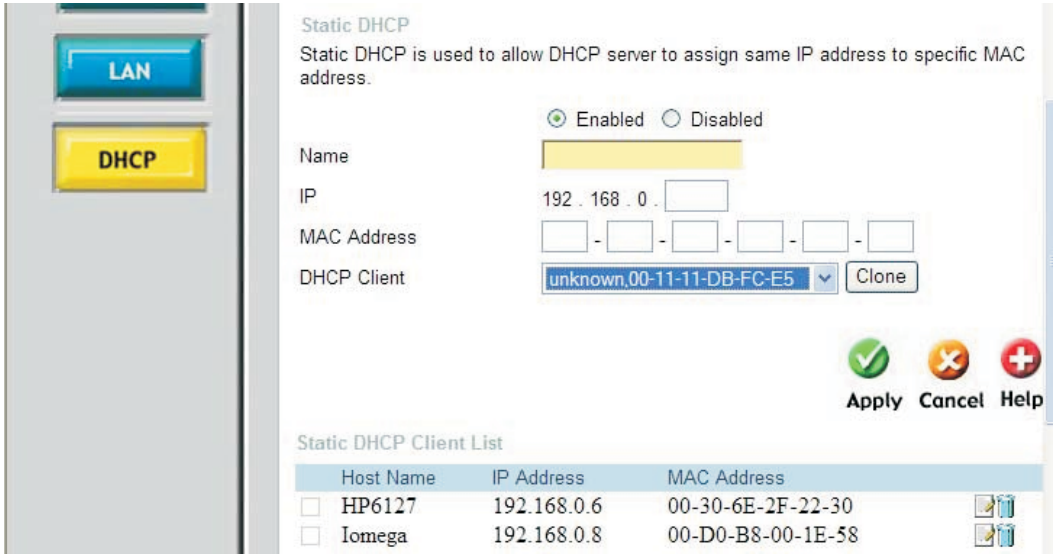
Define MAC addresses that can access the network

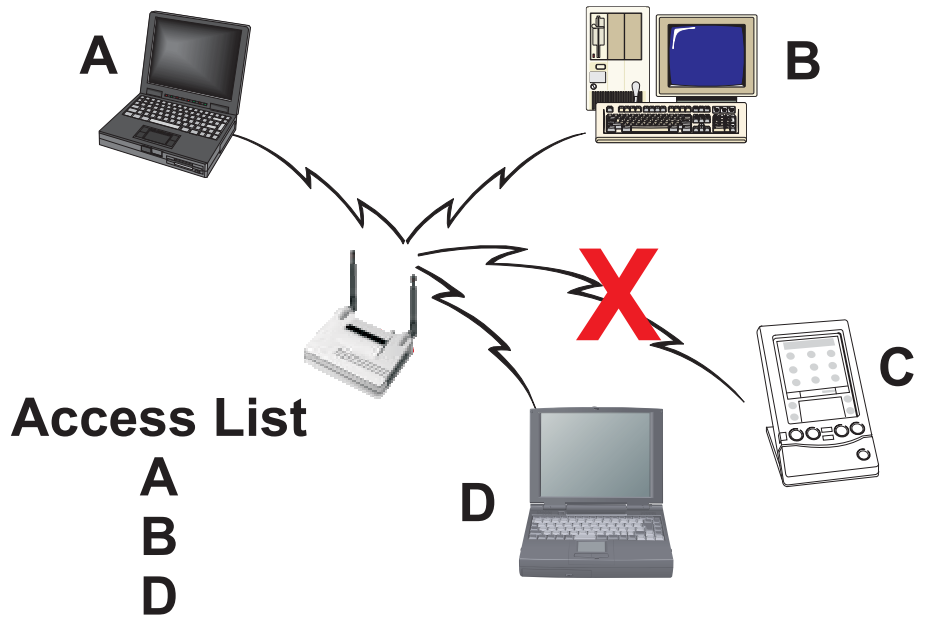
Must compile, maintain, and distribute a list of valid MAC addresses to all APs

Administratively intensive for large networks

If you do not have many visitors with PCs, this works well at home

Address spoofing difficult but not impossible





Agenda

Introduction

SSID

MAC ID

WEP

802.1x

WPA

VPN

VLAN

Summary

WEP - Wired Equivalent Privacy

Designed to be computationally efficient, self-synchronizing, and portable

All devices using a given AP use the same encryption key
- **Multiple concurrent keys supported**

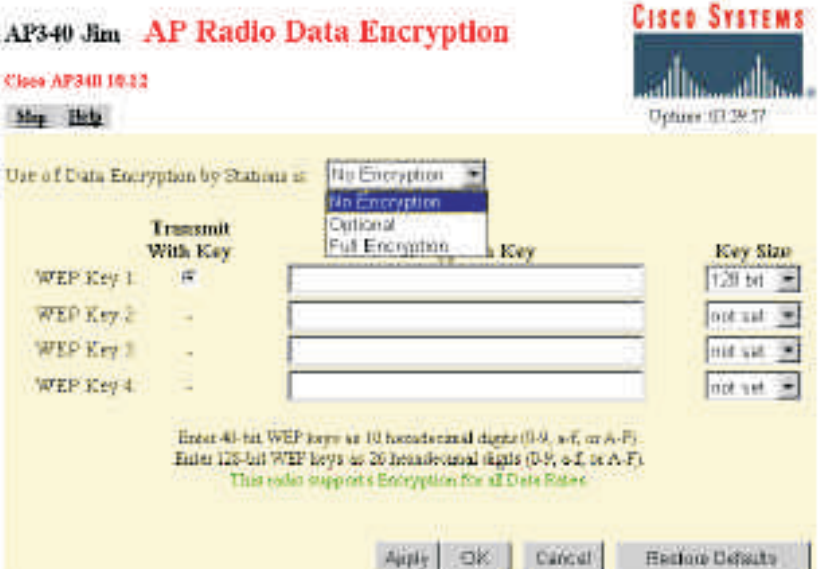
Data headers remain unencrypted

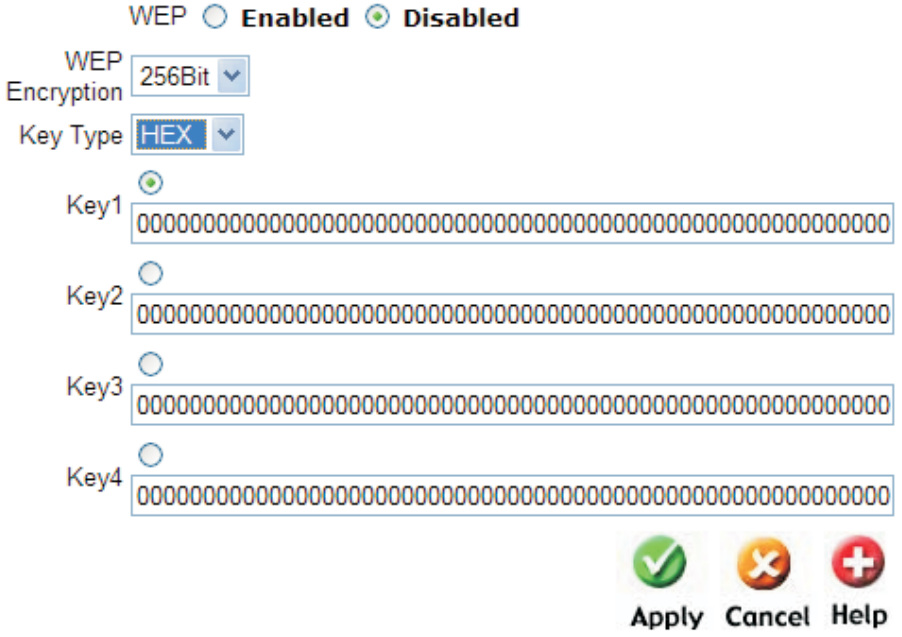
Goals:

- **Bring security level of wireless LANs close to that of wired LANs**
- **Protect confidentiality of user data**
- **Control network access**

Two subsystems:

- **Data encapsulation technique called WEP**
- **Authentication algorithm called Shared Key Authentication**





WEP and Shared Key Authentication

Send a management frame with an authentication request

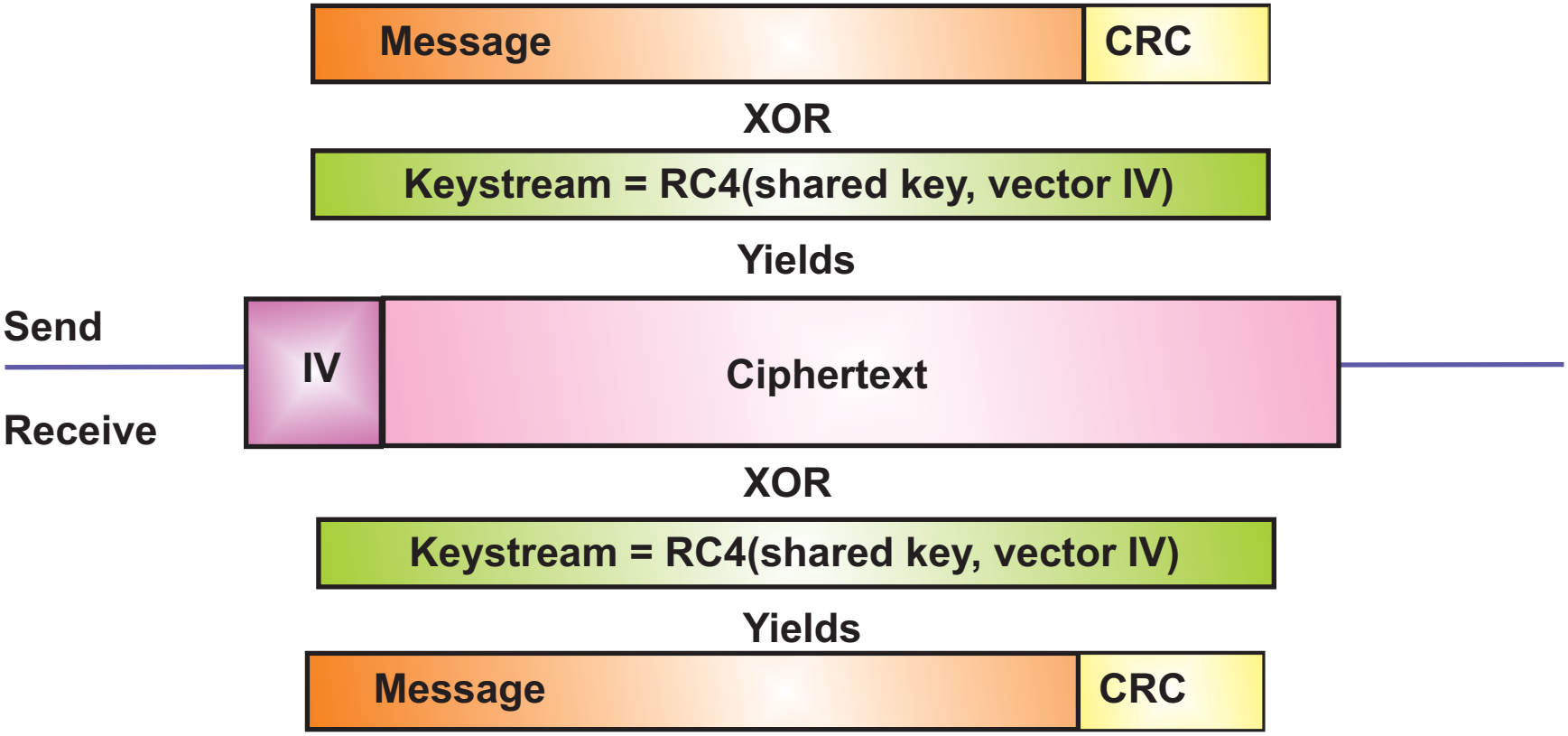
Respond with 128 octets of challenge text generated with WEP pseudo-random number generator with the shared secret key and a random initialization vector (IV)

Copy the challenge text into a new management frame body. Encrypt using the shared secret key along with the new IV

Is the CRC correct? Does the challenge text match the text sent? If yes, AP authenticated

Then send a management frame to station with an authentication request and repeat the process to authenticate station

WEP Pictorially



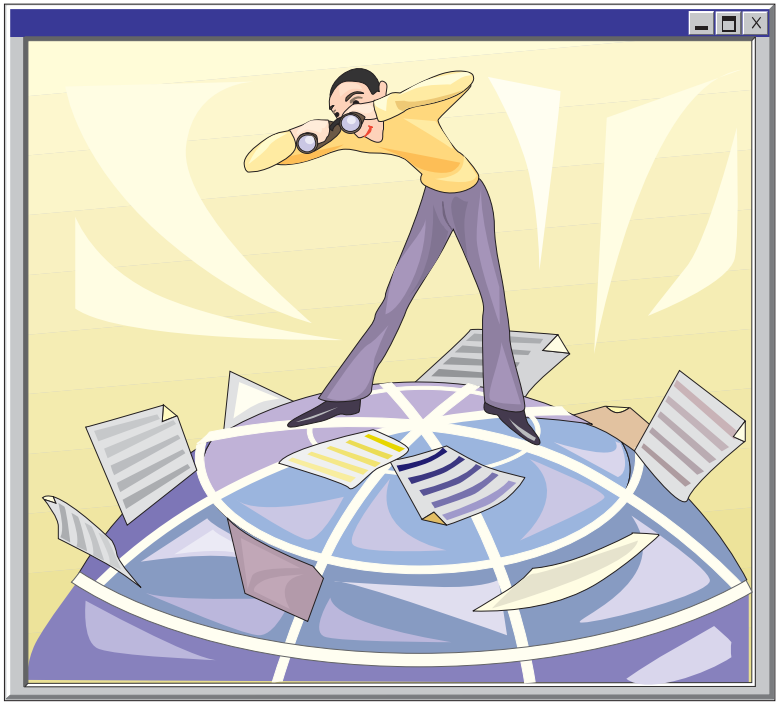
XOR the keystream with the plaintext to get the ciphertext

At the receiving side, the receiver generates the same keysteam (now that it has the IV component) and XORs the ciphertext to get the original message

The XORs cancel each other out

Wireless LAN Holes

802.11 uses WEP (Wired Equivalent Privacy) for security
- 64, 128, or 256 bit key
- RC4 stream cipher



One Scenario
- a) Attacker eavesdrops on wireless traffic, learns addresses
- b) Sends a plain-text packet to a legitimate station address
- c) The AP encrypts the packet and relays to the destination
- d) Attacker intercepts the encrypted packet and compares it to original plain-text message, allowing key to be deduced

AirSnort - Downloadable tool that automates this attack

Current devices support WPA, or WEP can be used in conjunction with other security measures such as IPSec or other VPN technology

Wireless scanners available to discover security flaws

TKIP

Temporal Key (TK) Integrity Protocol
Temporary, limited by time

Firmware upgrade to existing hardware

Fixes reuse of encryption keys by WEP

128 bit temporal key (TK) shared among clients and AP

TK plus MAC Address plus 16 octet IV make up encryption key

Each station uses a different key

Uses RC4 but changes key every 10,000 packets

Ultimate solution is AES (Advanced Encryption Standard) in the hardware...but this requires hardware change

Agenda

Introduction

SSID

MAC ID

WEP

802.1x

WPA

VPN

VLAN

Summary

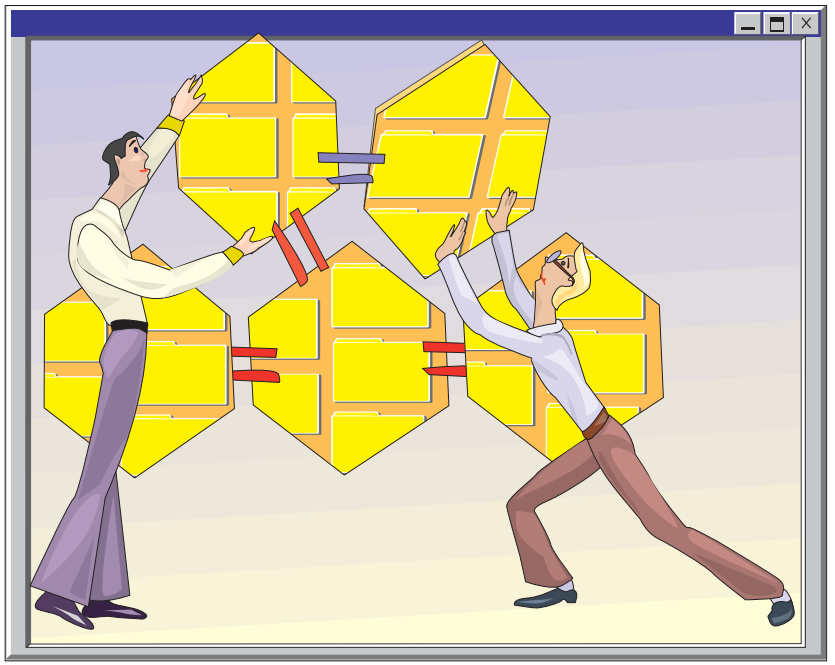
802.1x

Standard for wired LAN security approved in 1991

Enhancements for wireless
approved in 2004

Port based network access
control

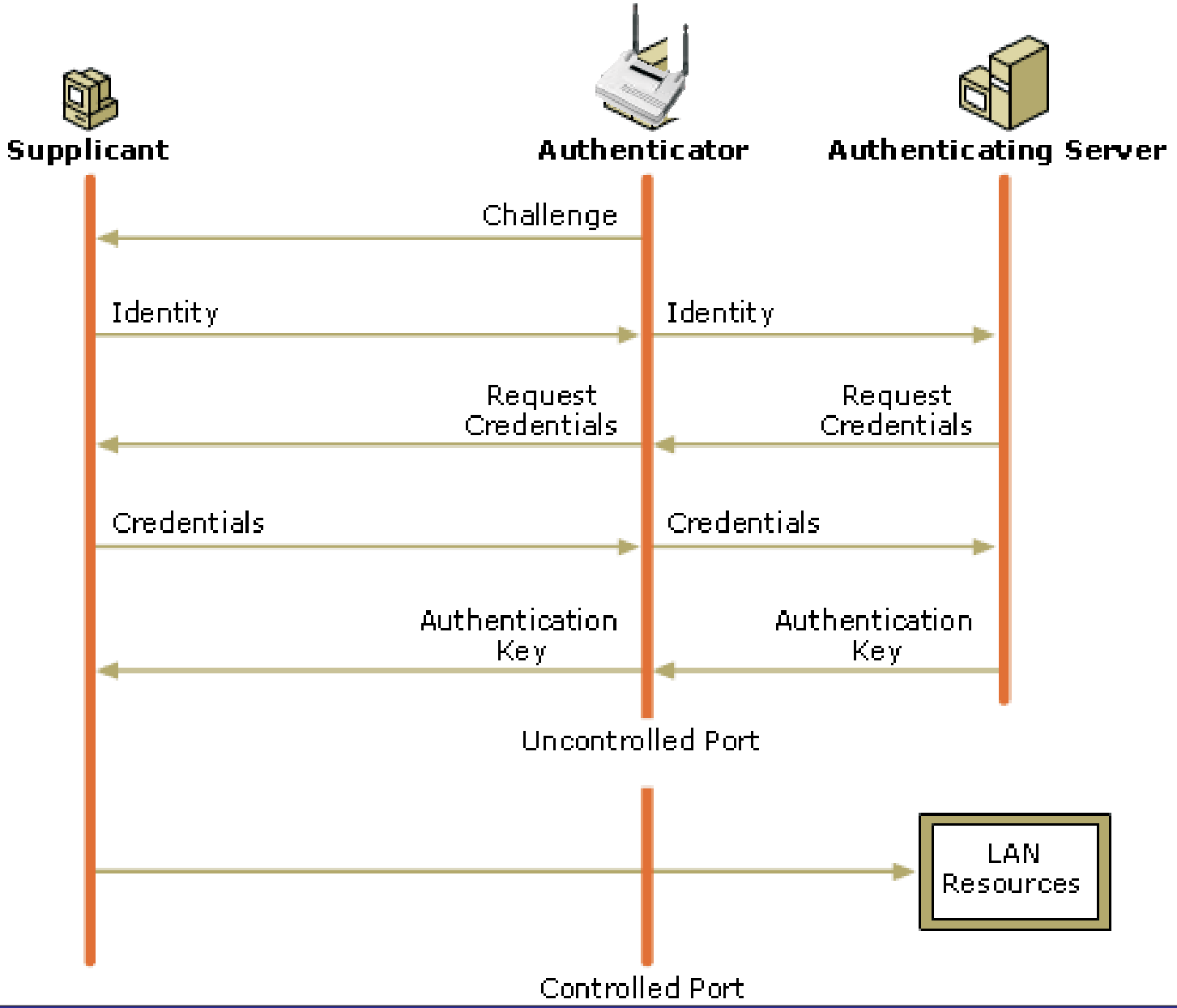
Uncontrolled port access
Before authentication complete,
only communication is to
authentication server
(usually a RADIUS server)



Controlled port access
Devices that have been successfully authenticated
communicate with anyone

Uses EAP (Extensible Authentication Protocol)
in one of its flavors

802.1x Authentication



802.1x and EAP Variations

EAP - Extensible Authentication Protocol

LEAP - Lightweight EAP
Password based

EAP-TLS - Transport Layer Security
Certificate based

EAP-TTLS - Tunneled Transport Layer Security
Hybrid certificate/password based

PEAP - Protected EAP
Hybrid certificate/password based

EAP-FAST - Flexible Authentication via Secure Tunneling

802.1x Summary

Helps prevent

- Rogue Access Points
- Session hijacking
- Man in the middle
- Dictionary attack

EAP-TTLS and PEAP

- Both require CA but only for server
- No client certificate

EAP-FAST

- Easier to implement and supports roaming

Agenda

- Introduction
- SSID
- MAC ID
- WEP
- 802.1x
- WPA
- VPN
- VLAN
- Summary

WPA (WiFi Protected Access) Technologies

WPA = 802.1X + EAP + TKIP + MIC

User authentication
- 802.1X + EAP (Extensible Authentication Protocol)

Message encryption and authentication
- TKIP (Temporal Key Integrity Protocol)
- 802.1X server distributes dynamic key
- MIC (Message Integrity Check) a.k.a. Michael

SOHO applications use pre-shared key for both
- Because of difficulty, Wi-Fi Alliance standardized
  - WPS - Wireless Protected Setup
    - Connect the device to the AP and authenticate
    - Sort of plug and play

WEP and WPA Comparison

	WEP	WPA
Encryption	Flawed, cracked by scientists and hackers	Fixes WEP's flaws
Key length	40,64,128-bit keys	128-bit keys
Key sharing	Static key – same key used by everyone on the network	Dynamic session keys. Per user, per session, per packet keys
Key source	Manual distribution of keys– hand typed into each device	Automatic distribution of keys
Authentication	Flawed, used WEP key itself for authentication	Strong user authentication, utilizing 802.1x and EAP

IEEE 802.11i Security aka WPA2

PTK = AES block cipher of
Pairwise Master Key +
AP nonce + Station nonce +
AP MAC + Station MAC

AP nonce

PTK is Pairwise Temporal (Transient) Key

Station constructs PTK

Station nonce + MIC

Message Identification Code
(Message Authentication Code)

AP constructs PTK

Group Temporal Key + MIC

ACK

WPA and WPA2 Comparison

	WPA	WPA2
Enterprise		
Authentication	802.1x/EAP	802.1x/EAP
Encryption	TKIP/MIC	AES/CCMP
SOHO and Personal		
Authentication	PSK	PSK
Encryption	TKIP/MIC	AES/CCMP

Agenda

Introduction

SSID

MAC ID

WEP

802.1x

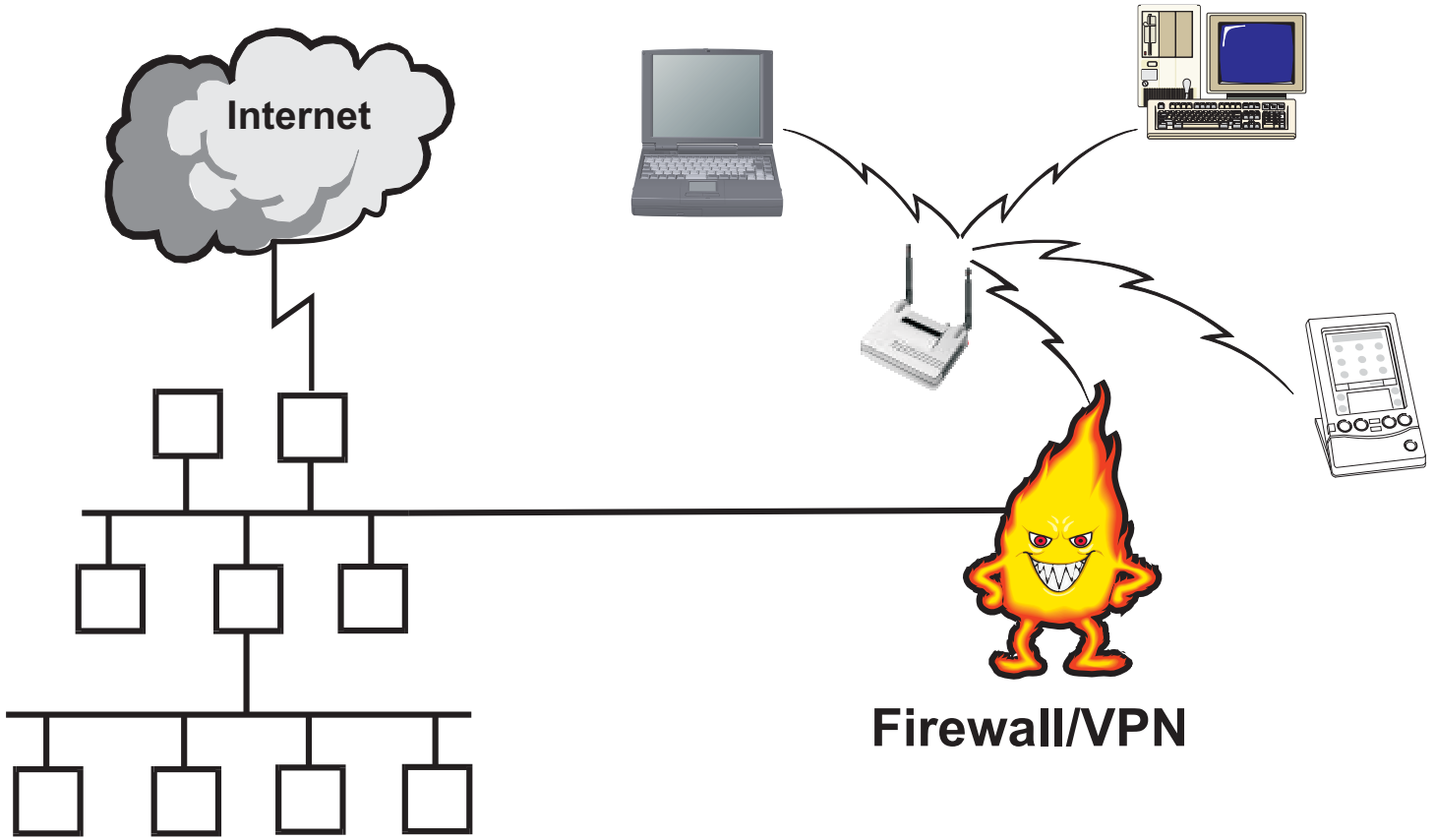
WPA

VPN

VLAN

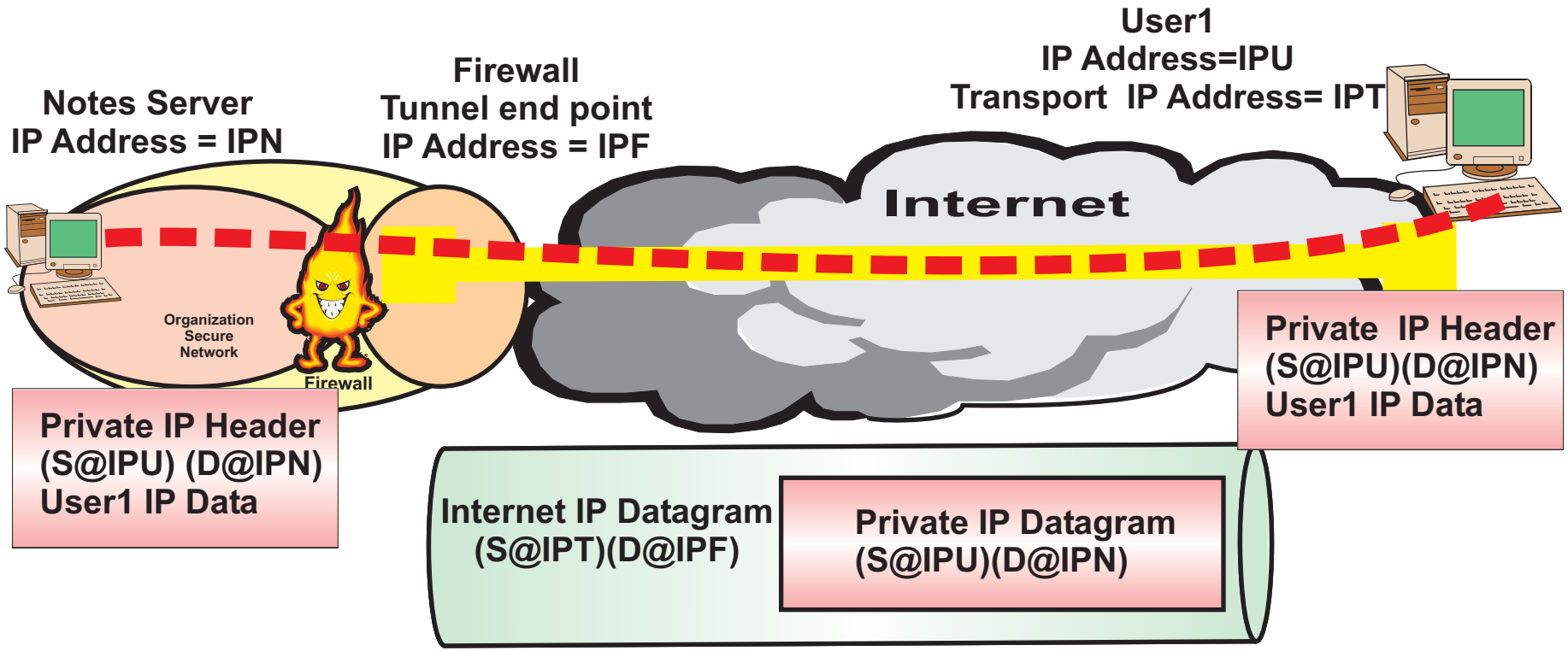
Summary

VPN - Virtual Private Network



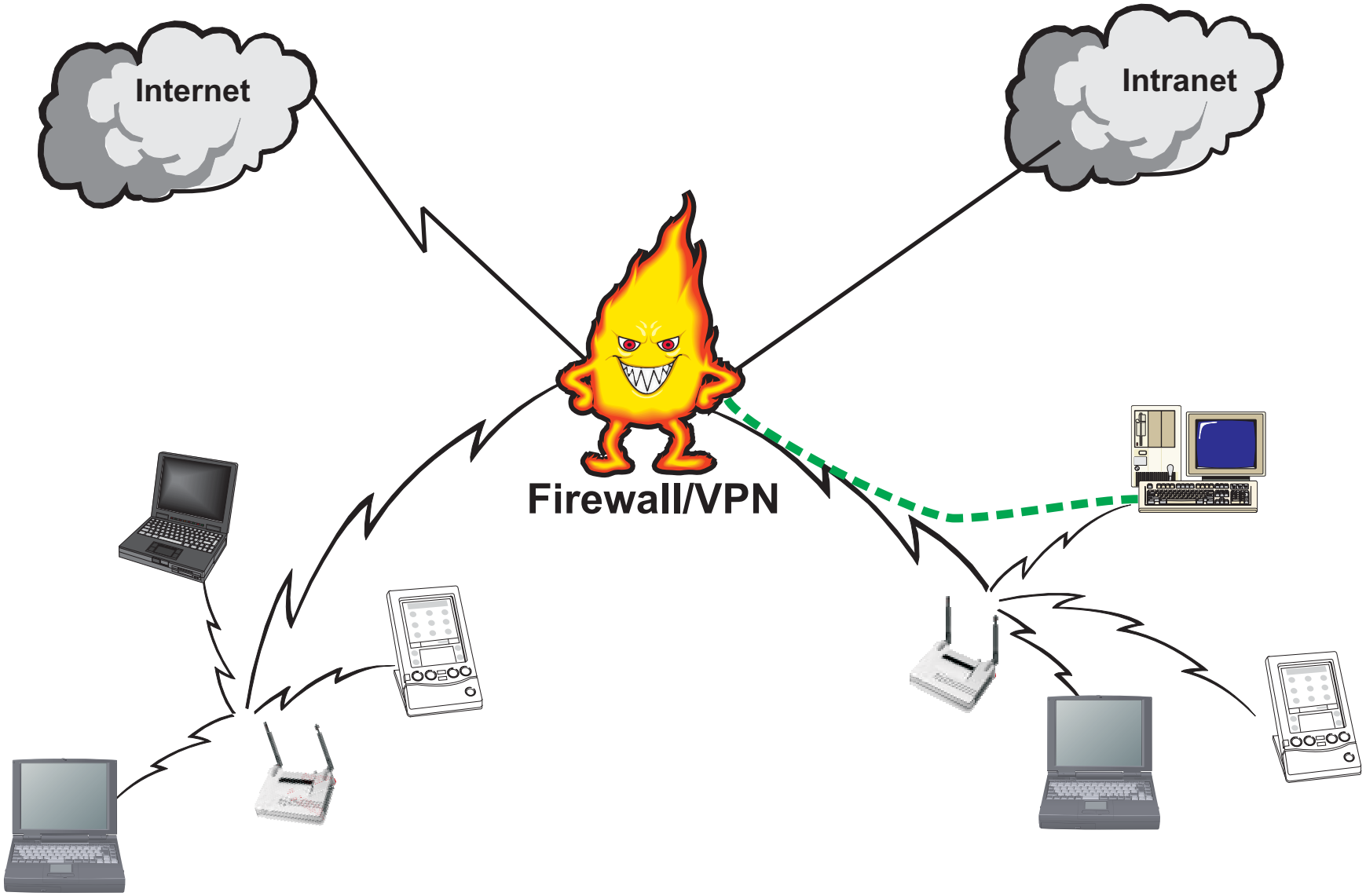
Scalable authentication and encryption solution
Requires end user configuration and VPN software
Requires end user knowledge of VPN technology
User re-authenticates if roaming

How VPNs Work



Tunneling includes
encapsulation
transmission
un-encapsulation

VPN and Wireless LANs



Agenda

Introduction

SSID

MAC ID

WEP

802.1x

WPA

VPN

VLAN

Summary

VLAN - Virtual Local Area Networks

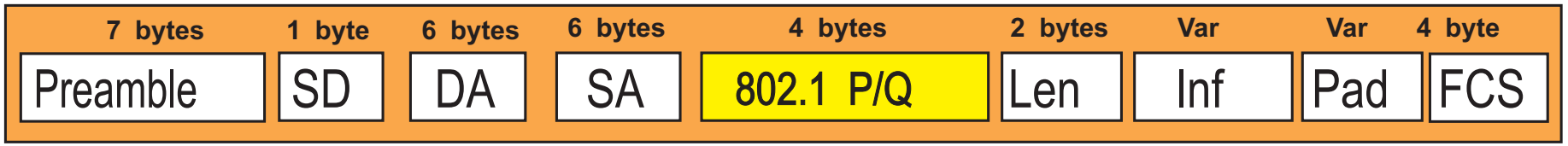
Good for enterprise LANs

Reconfiguring WEP keys difficult

Have multiple access points and subnets

Combine wireless networks on one VLAN even if geographically separated

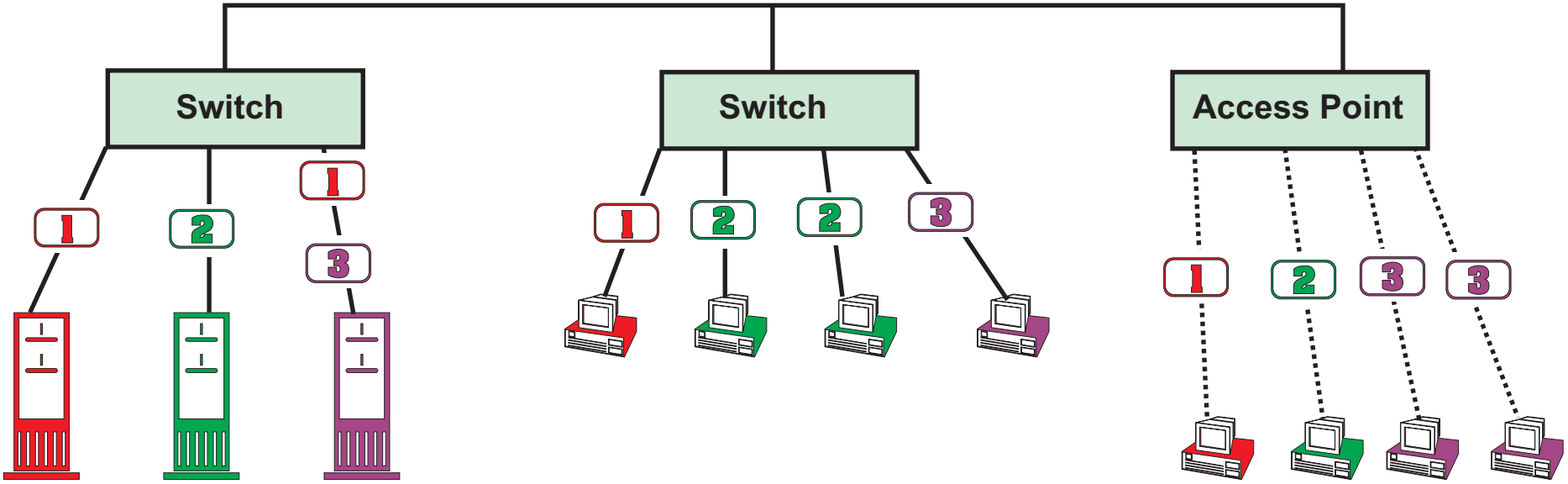
Use 802.1Q VLAN tagging to create a wireless subnet and a VPN gateway for authentication and encryption



802.1Q header
- TPI : Tag protocol identifier
- VI : VLAN identifier

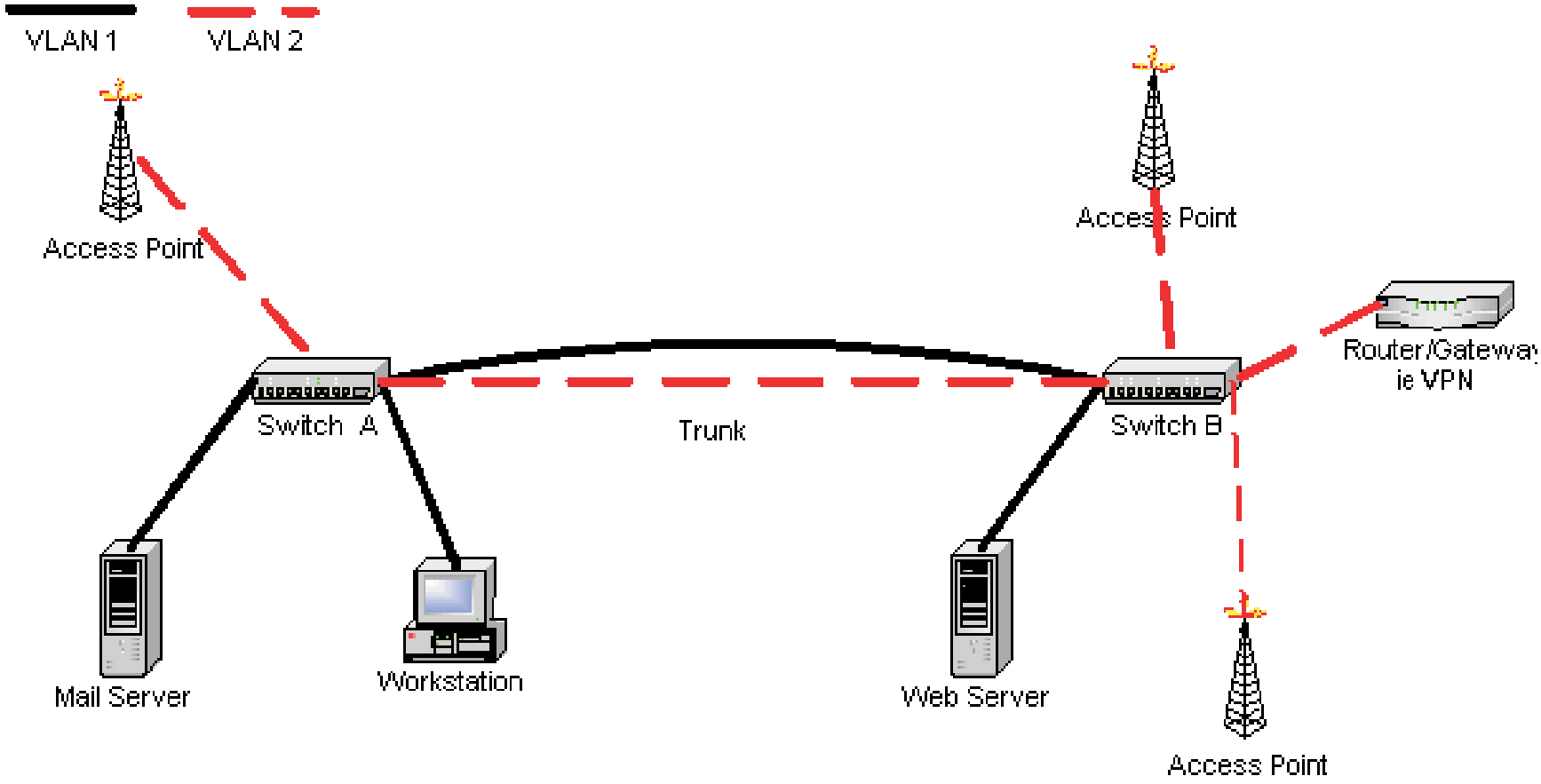
802.1P header
- P : Priority
- C : Canonical format indicator

Anatomy of a VLAN



Manages broadcast domains
Users and access ports are uniquely assigned to a VLAN
Physical location no longer determines LAN association
Need to balance benefits with administration requirements
Scalable (but adminstratively rich)

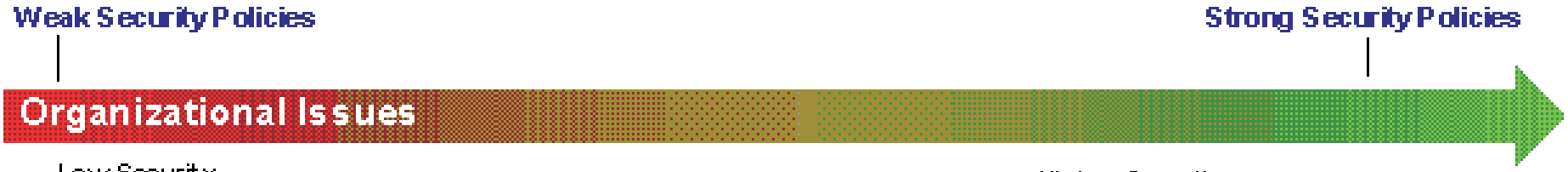
VLANs and WLAN



Wireless Security Review

Low Security
- Little Access Control
- Easy for Hackers to link into the Network
- Addresses can be spoofed

Higher Security
- Controlled and secure environment
- Access Control
- Increased Granularity
- Additional hardware, software and management
- Client Access control
- Better Manageability



Low Security
- Employee installed access points
- Inability to identify rogue acess points

Higher Security
- Security policies enforced
- Employees educated about security
- Periodic security health checks

* and variations like EAP, EAP-TTLS, PEAP

Wireless LAN Security Tips

Change the default login name and password on Access Point
(this includes the web interface)
Change the default SSID (network name)
Disable the SSID broadcast option
Enable MAC address filtering on your Access Point
Restrict DHCP leases to the MAC addresses
of your Wireless clients only
Choose random subnet address (not the default)
Use the highest level of WEP/WPA/WPA2
Firewall your wireless network segment
(separate segment and packet filtering)
Connect the Access Point to the rest of the network with a switch
Encrypt your wireless traffic using a VPN
Further, use encryption protocols for applications where possible
(TLS/https, ssh, etc)
Think about using a proxy with access control for outgoing requests
Enable logging, and check your log files regularly
Test your wireless security using wardriving tools

Summary

Wireless LANs very attractive

Default security not adequate for sensitive environments

Can be secured with careful planning and administration

Growing use and popularity has resulted in stronger and easier to implement security protocols

Just as we grew into security in wired LANs, we can now implement secure wireless LANs

References

Cisco (Good source of technical articles) ..... www.cisco.com
Computer Emergency Response (US funded at CMU) ..... www.cert.org
PGP (Pretty Good Privacy) ..... www.pgp.com
RSA Security (Secure ID) ..... www.rsasecurity.com
Secure Computing Corp. (Corporate level) ... www.securecomputing.com

Guides, How-to, News ..... www.practicallynetworked.com

Applied Cryptography 2nd Ed, Schneier, 1995; ISBN: 9780471117094
Network Security, Private Communication in a Public World
2nd Ed, 2002; ISBN: 0130460192
Network Security Fundamentals, Cisco Press, 2005; ISBN: 9781587051678
802.11 Wireless Networks: The Definitive Guide, 2nd Edition,
Matthew Gast, O'Reilly, 2005
Take Control of Your Wi-Fi Security, O'Reilly, 2007

08/2009

Acronyms 1

802.1x	IEEE Committee Standardizing Access Control Security
802.11i	IEEE Committee Standardizing Wi-Fi Security
ACK	Acknowledgment
AES	Advanced Encryption Standard
AP	Access Point
BSS	Basic Service Set
CCMP	Counter-mode Cipher block chaining Message authentication code Protocol
CRC	Cyclical Redundancy Check
CSMA/CA	Carrier Sense Multiple Access with Collision Avoidance
CTS	Clear to Send
EAP	Extensible Authentication Protocol
FAST	Flexible Authentication via Secure Tunneling
IBSS	Independent Basic Service Set
IPSec	Internet Protocol Security
IV	Initialization Vector
LAN	Local Area Network
LEAP	Lightweight Extensible Authentication Protocol
MAC ID	Media Access Control Identifier
MIC	Message Integrity Code (Authentication outside networking)
nonce	Single use number

Acronyms 2

PAC	Protected Access Credentials
PEAP	Protected Extensible Authentication Protocol
PMK	Pairwise Master Key
PTK	Pairwise Temporal (or Transient) Key
RADIUS	Remote Authentication Dial-In User Service
RC4	Rivest Cipher #4 (Stream Cipher)
RSN	Robust Security Network
RTS	Request to Send
SSID	Service Set Identifier
SOHO	Small Office / Home Office (Market Segment)
TKIP	Temporal Key Integrity Protocol
TLS	Transport Layer Security
TSN	Transition Security Network
TTLS	Tunneled Transport Layer Security
VLAN	Virtual Local Area Network
VPN	Virtual Private Network
WEP	Wired Equivalent Privacy
Wi-Fi	Wireless Fidelity (Industry Interoperability)
WLAN	Wireless Local Area Network
WPA	Wi-Fi Protected Access
WPS	Wireless Protected Setup
XOR	Exclusive Or (Logical Operator)