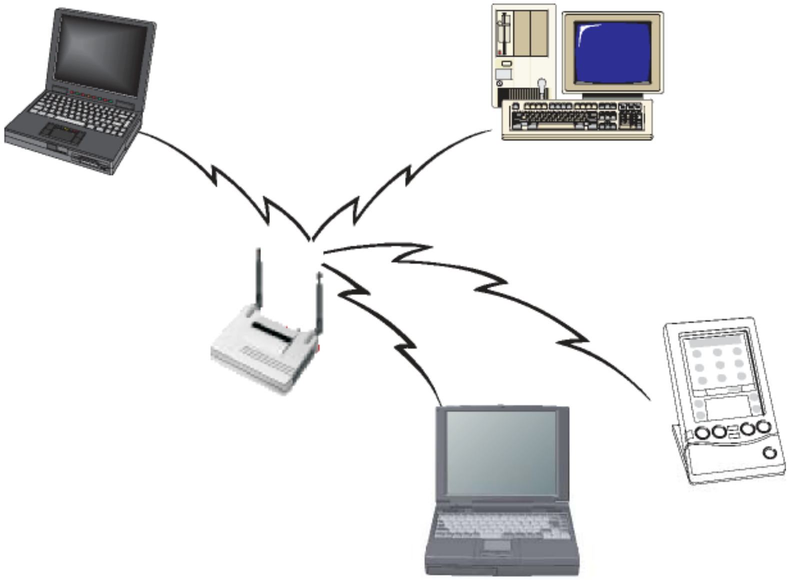
Wireless Network Security Challenges

SHARE Summer 2010 Boston

Laura Knapp
WW Business Consultant
Applied Expert Systems (www.aesclever.com)
laurak@aesclever.com
laura@lauraknapp.com

Wireless is NOT Secure

Any questions?



Thank you, have a nice day!

Agend

Introduction

SSID

MAC ID

WEP

802.1x

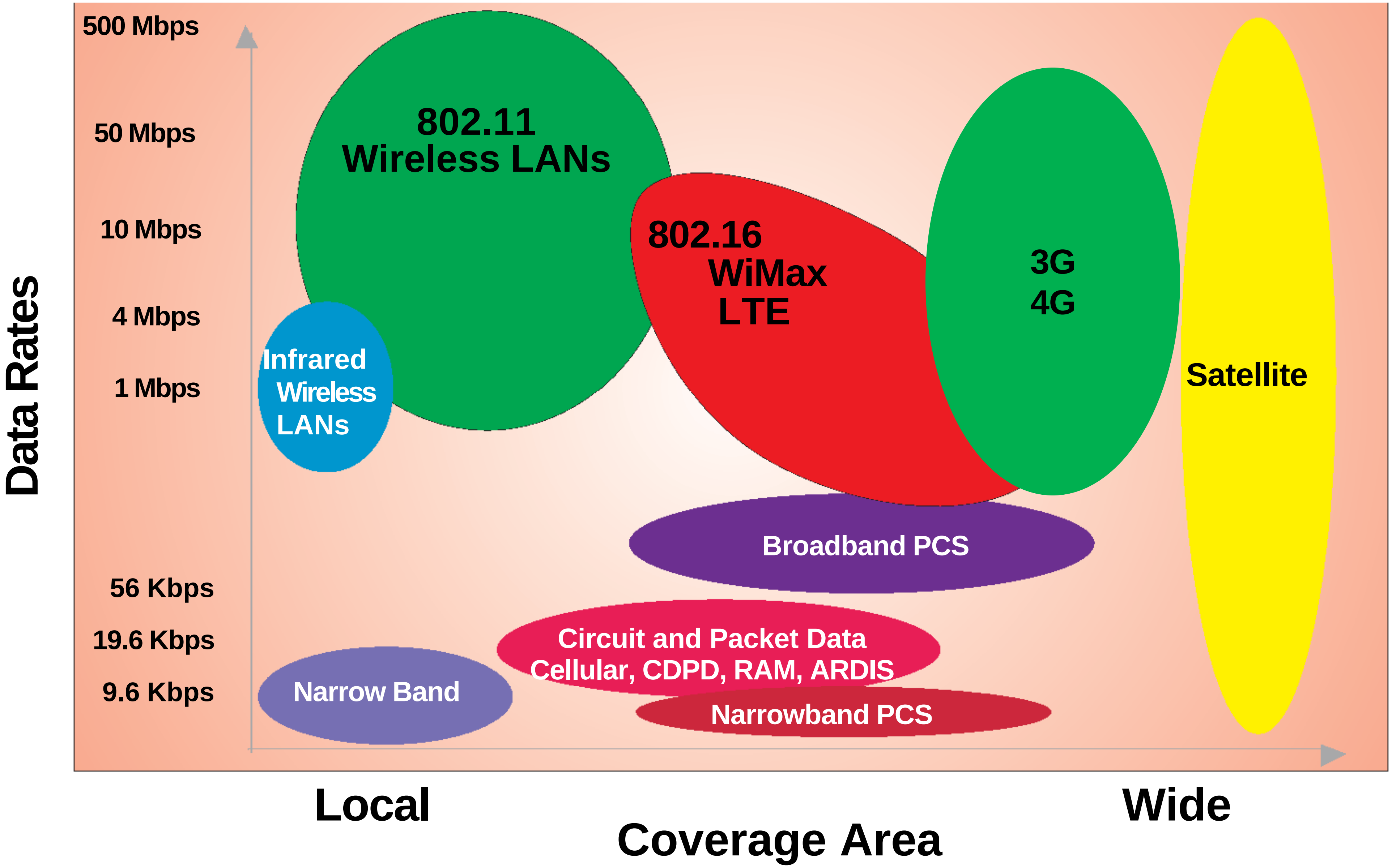
WPA

VPN

VLAN

Summary

Wireless Technologies



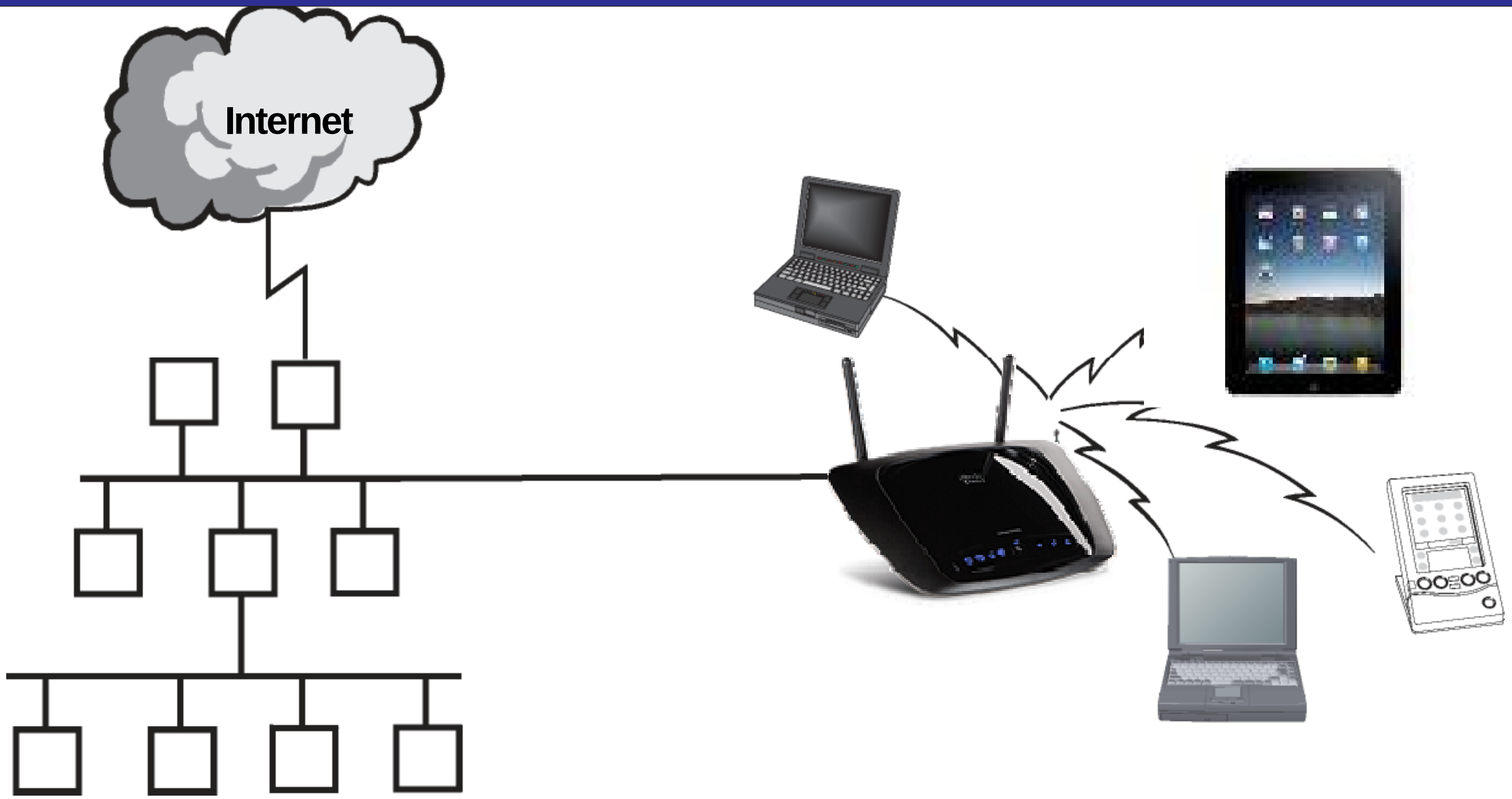
Wireless LAN Technologies

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	OFDM (MIMO/SDM)
11 Mbps	54 Mbps	54 Mbps	Up to 600 Mbps

The Laws of Radio Dynamics:

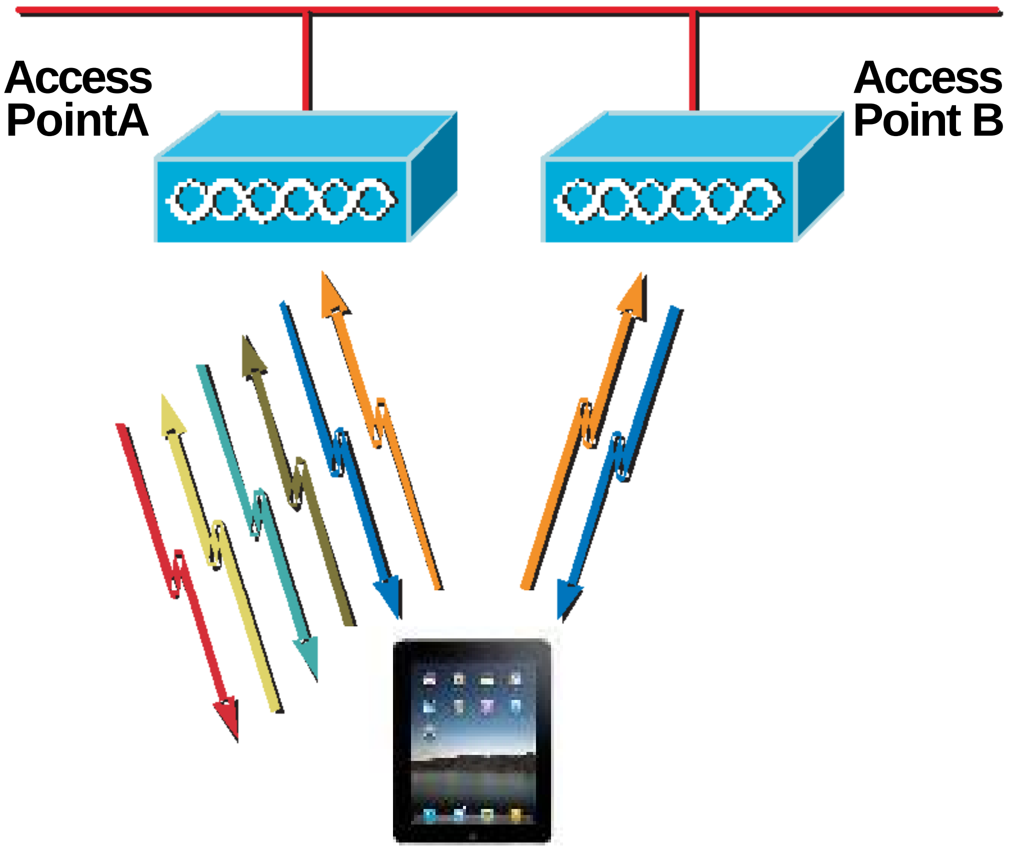
Higher data rates = shorter transmission range
Higher power output = increased range, but lower battery life
Higher frequency radios = higher data rates, shorter ranges

Wireless LAN Topology



Security in wireless LANs has many elements:
Focus of this session
Securing Access
Securing Data

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

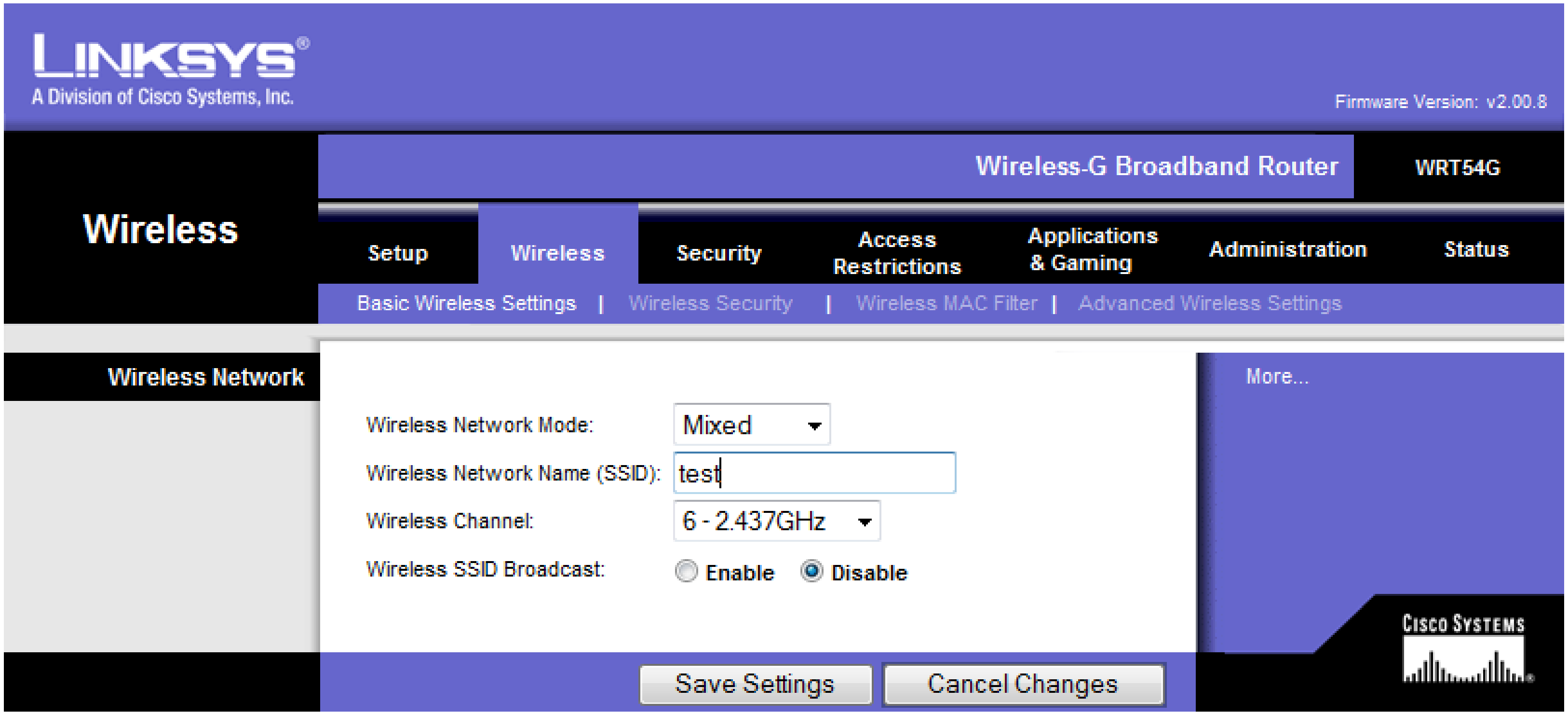
WPA

VPN

VLAN

Summary

SSID - Service Set ID


LINKSYS®
A Division of Cisco Systems, Inc.
Firmware Version: v2.00.8
Wireless-G Broadband Router
WRT54G
Wireless
Setup
Wireless
Security
Access Restrictions
Applications & Gaming
Administration
Status
Basic Wireless Settings | Wireless Security | Wireless MAC Filter | Advanced Wireless Settings
Wireless Network
More...
Save Settings
Cancel Changes
Cisco Systems

Wireless Network Mode: Mixed

Wireless Network Name (SSID): test

Wireless Channel: 6 - 2.437GHz

Wireless SSID Broadcast: ○ Enable ● Disable

All Access Points have a defaul SSID….be sue and change it

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 (if you disable broadcast)

Agenda

SSID

MAC ID

WEP

802.1x

WPA

VPN

VLAN

Summary

MAC ID

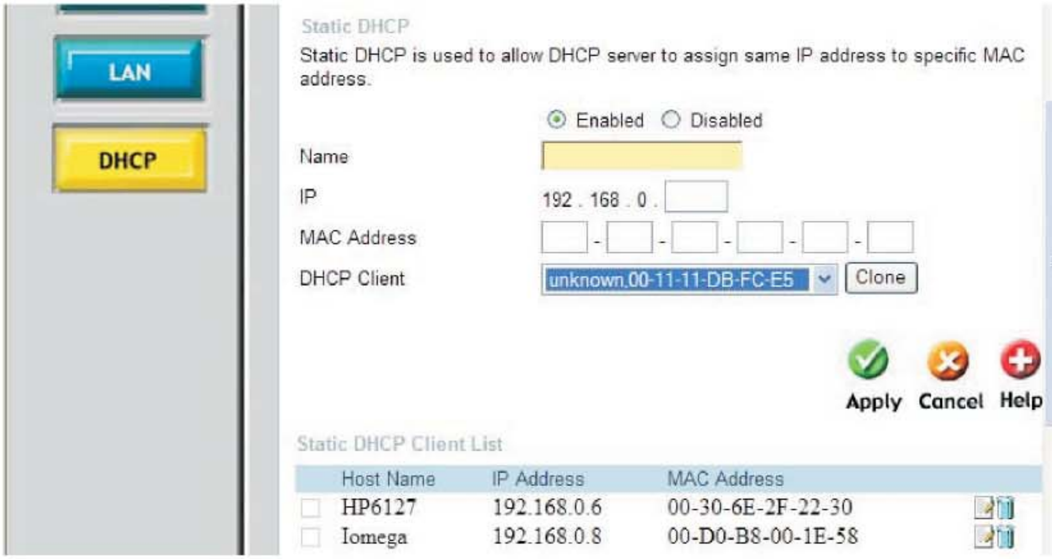
Define MAC addresses that can access the network

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



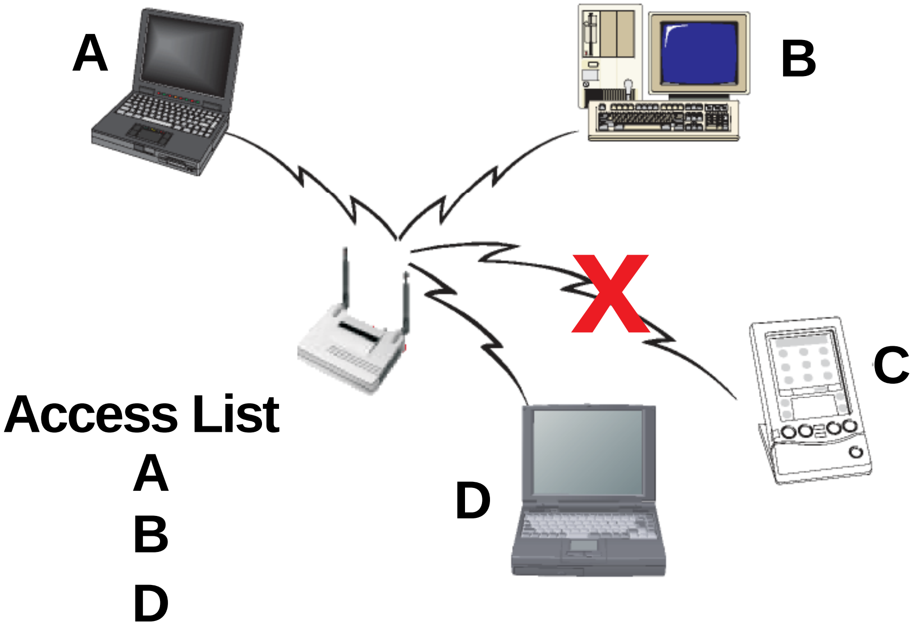
Static DHCP

Static DHCP is used to allow DHCP server to assign same IP address to specific MAC address.

	● Enabled ○ Disabled
Name	
IP	192 . 168 . 0 .
MAC Address	- - - - -
DHCP Client	unknown,00-11-11-DB-FC-E5 Clone

Static DHCP Client List

	Host Name	IP Address	MAC Address
□	HP6127	192.168.0.6	00-30-6E-2F-22-30
□	Iomega	192.168.0.8	00-D0-B8-00-1E-58



Access List
A
B
D

Agenda

SSID

MAC ID

WEP

802.1x

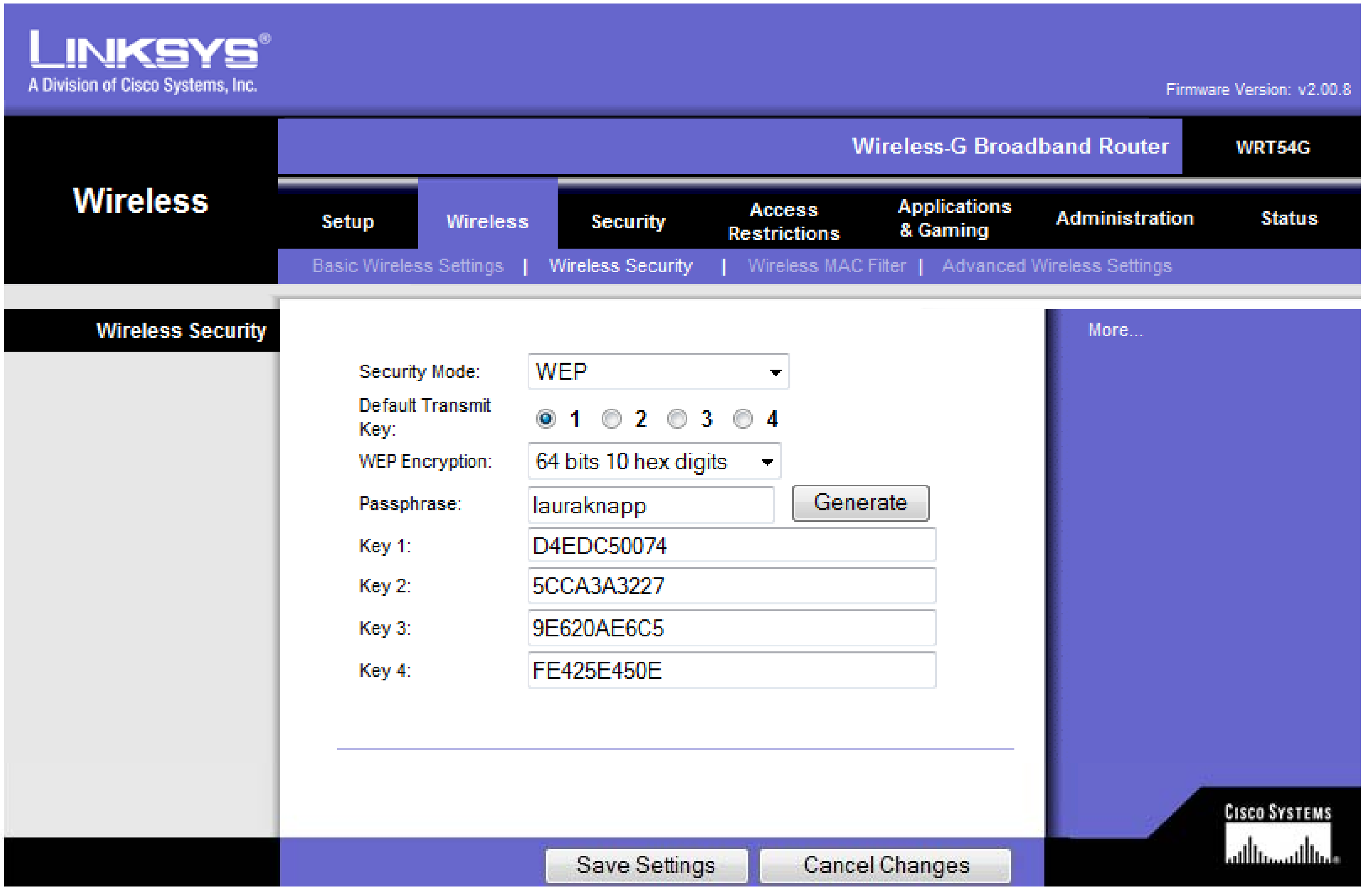
WPA

VPN

VLAN

Summary

WEP - Wired Equivalent Privacy

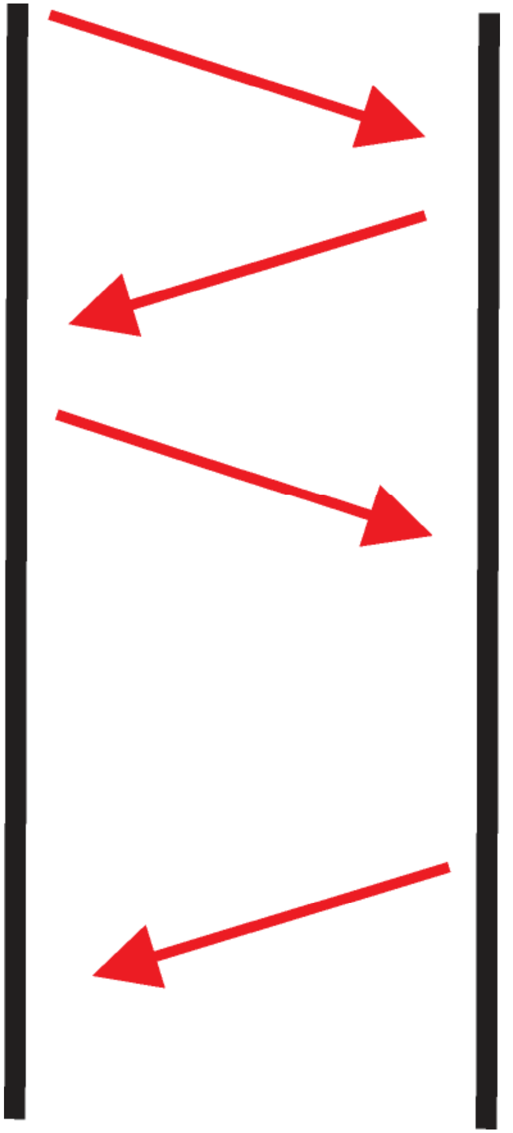

LINKSYS
A Division of Cisco Systems, Inc.
Firmware Version: v2.00.8
Wireless-G Broadband Router
WRT54G
Wireless
Setup
Wireless
Security
Access Restrictions
Applications & Gaming
Administration
Status
Basic Wireless Settings | Wireless Security | Wireless MAC Filter | Advanced Wireless Settings
Wireless Security
More...
Generate
Save Settings
Cancel Changes
Cisco Systems

Security Mode:	WEP
Default Transmit Key:	● 1 ○ 2 ○ 3 ○ 4
WEP Encryption:	64 bits 10 hex digits
Passphrase:	lauraknapp
Key 1:	D4EDC50074
Key 2:	5CCA3A3227
Key 3:	9E620AE6C5
Key 4:	FE425E450E

First privacy standard designed to give you the same functionality as a wired LAN

Got a bad name as it was ‘easily?’ hacked

Shared Key Authentication



Send a management frame with an authentication request

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

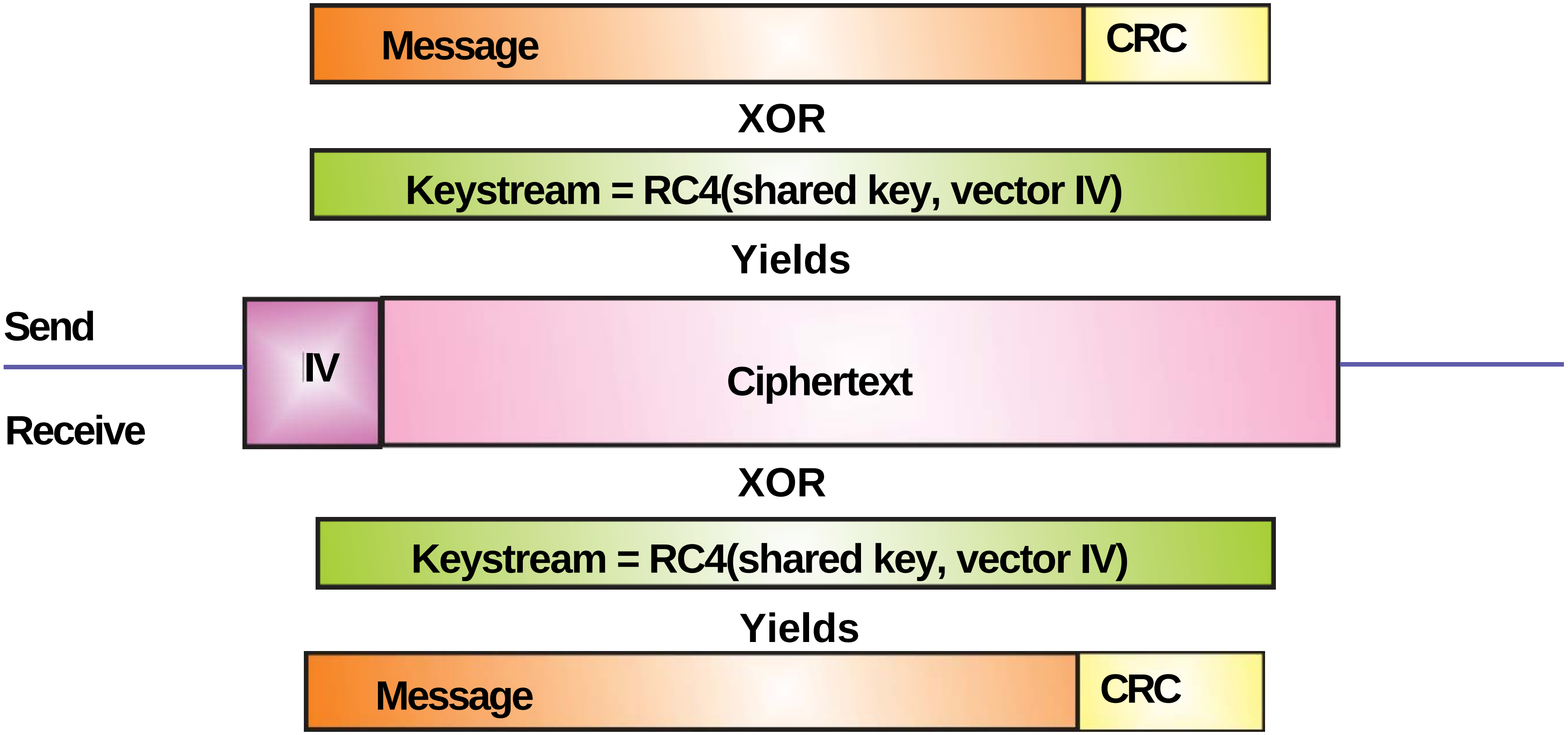
Respond with 128 octets of

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

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

WEP Problems


Message
CRC
XOR
Keystream = RC4(shared key, vector IV)
Yields
Send
IV
Ciphertext
Receive
XOR
Keystream = RC4(shared key, vector IV)
Yields
Message
CRC

Easily broken
All devices use the same ‘KEY’
Key is static
Initial keys were only 40 bits….but grew to 128 bits
Variations on WEP became available like WEP2, WEPplus and Dynamic WEP

Agenda

Introduction

SSID

MAC ID

WEP

802.1x

WPA

VPN

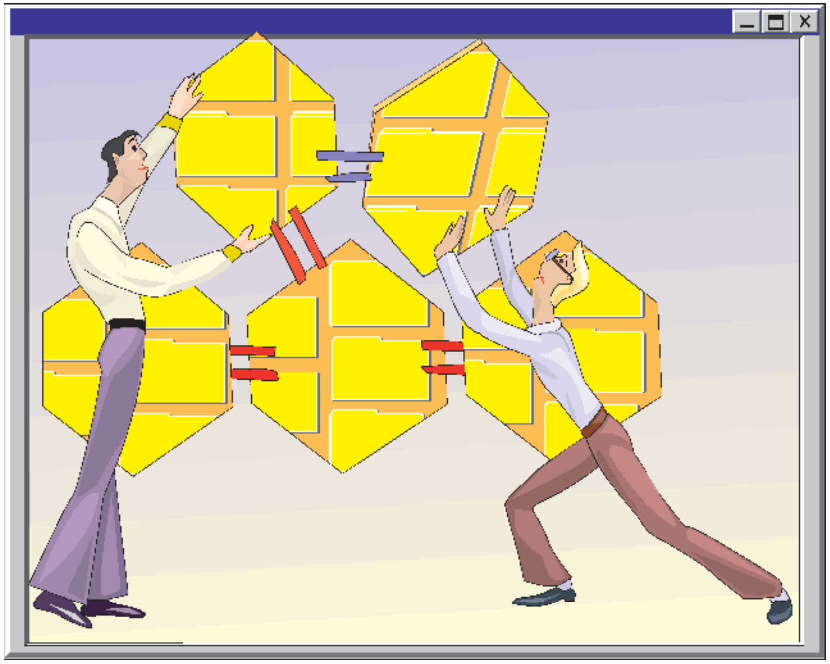
VLAN

Summary

802.1x

Standard for wired LAN/WAN security approved in 1991

Enhancements for wireless approved in 2004



Port based network access control

Uncontrolled port access

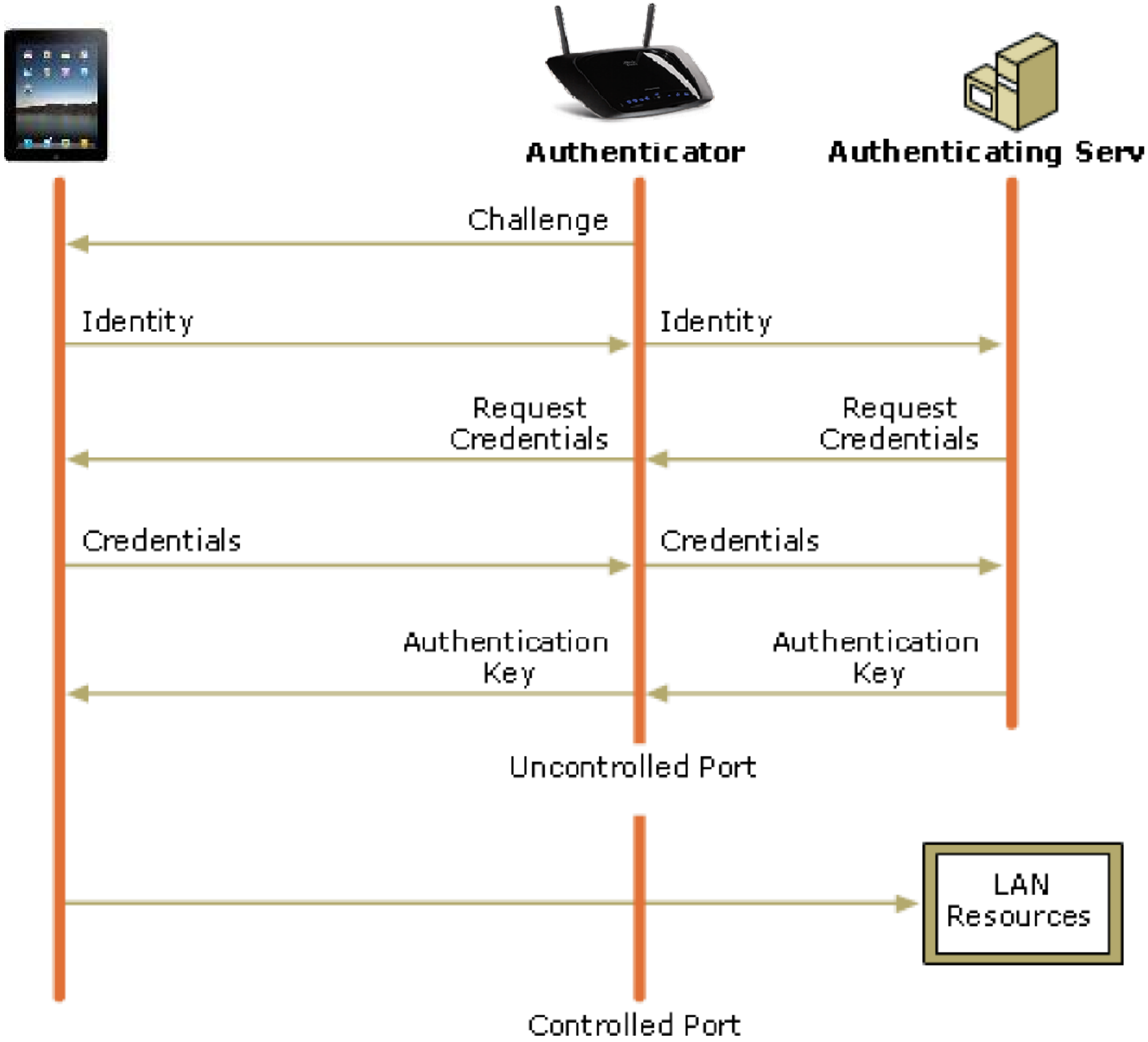
Before authentication complete, only communication is to authentication server (usually a RADIUS server)

Controlled port access

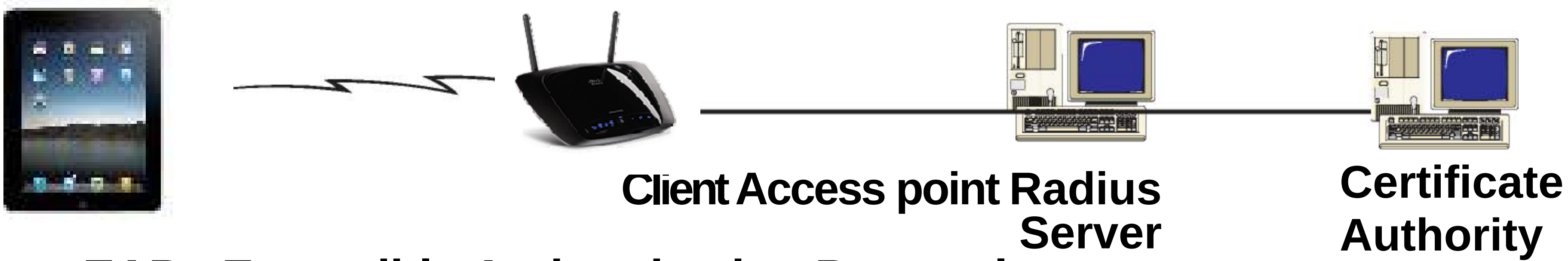
Devices that have been successfully authenticated communicate with anyone

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

802.1x Authentication



802.1x and EAP Variations



Client Access point Radius Server

Certificate Authority

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

Certificate Authority needed
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

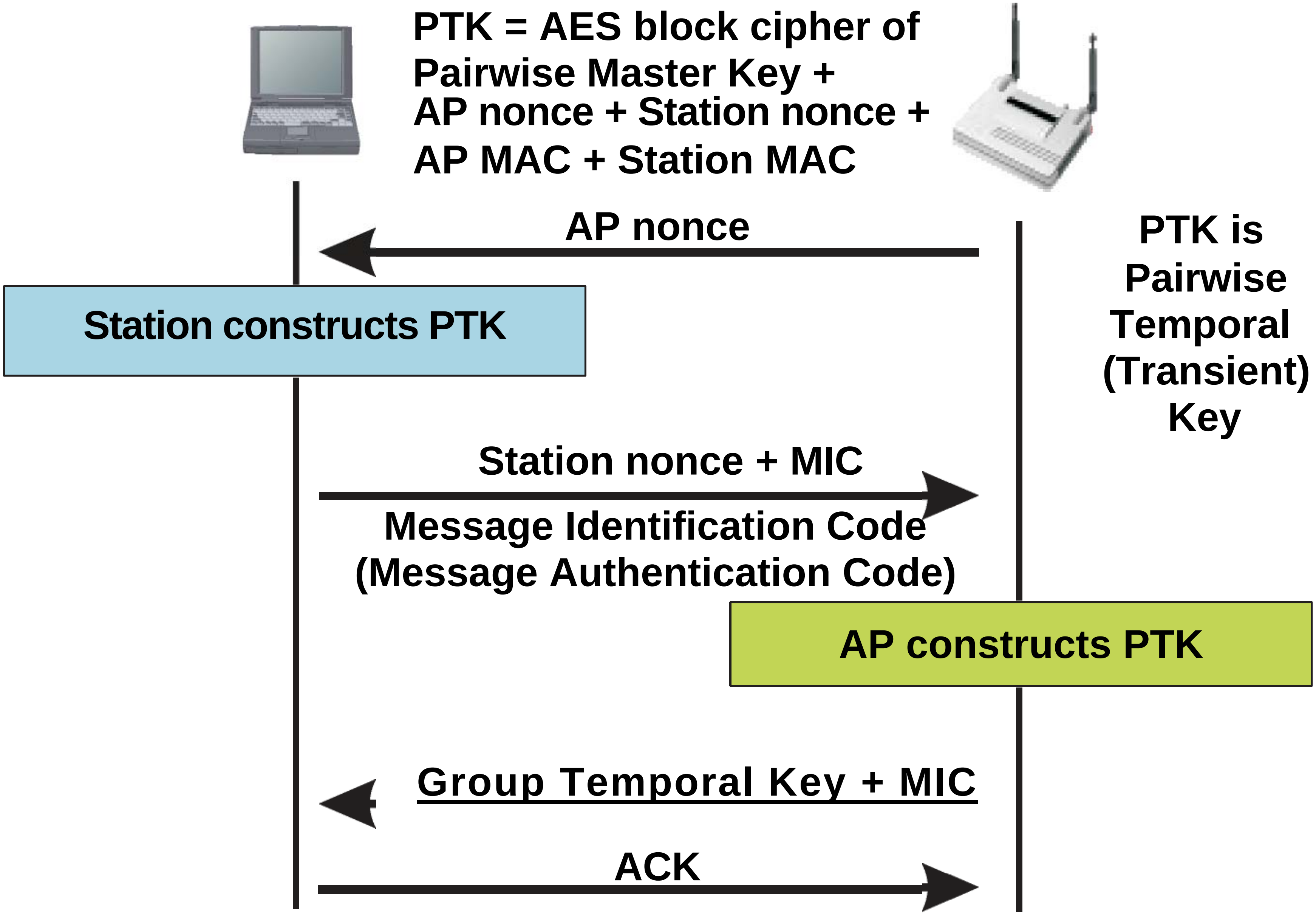
WPA = 802.1X + EAP + TKIP + MIC

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

IEEE 802.11i Security aka WPA2



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

AP nonce

Station constructs PTK

PTK is
Pairwise
Temporal
(Transient)
Key

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

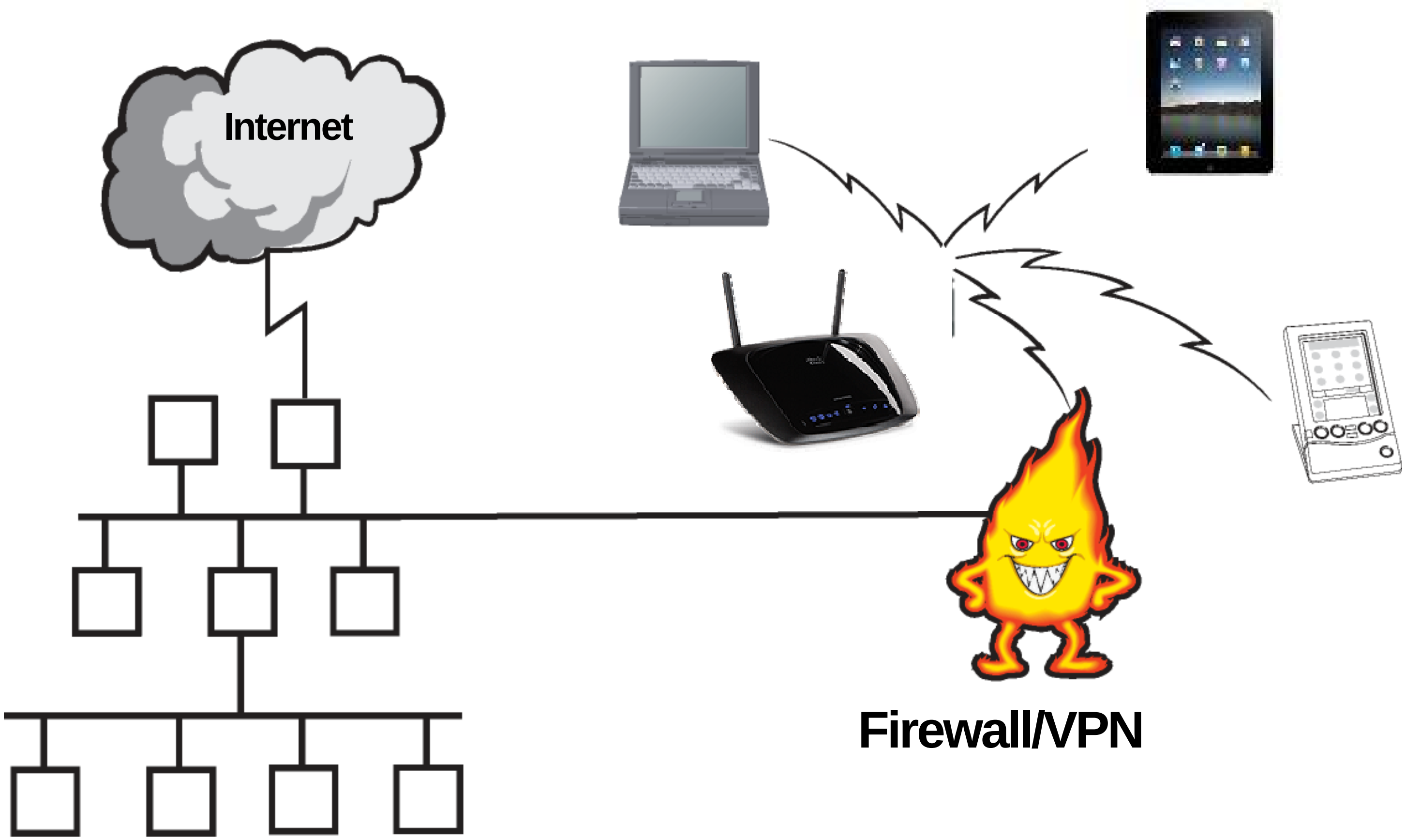
WPA

VPN

VLAN

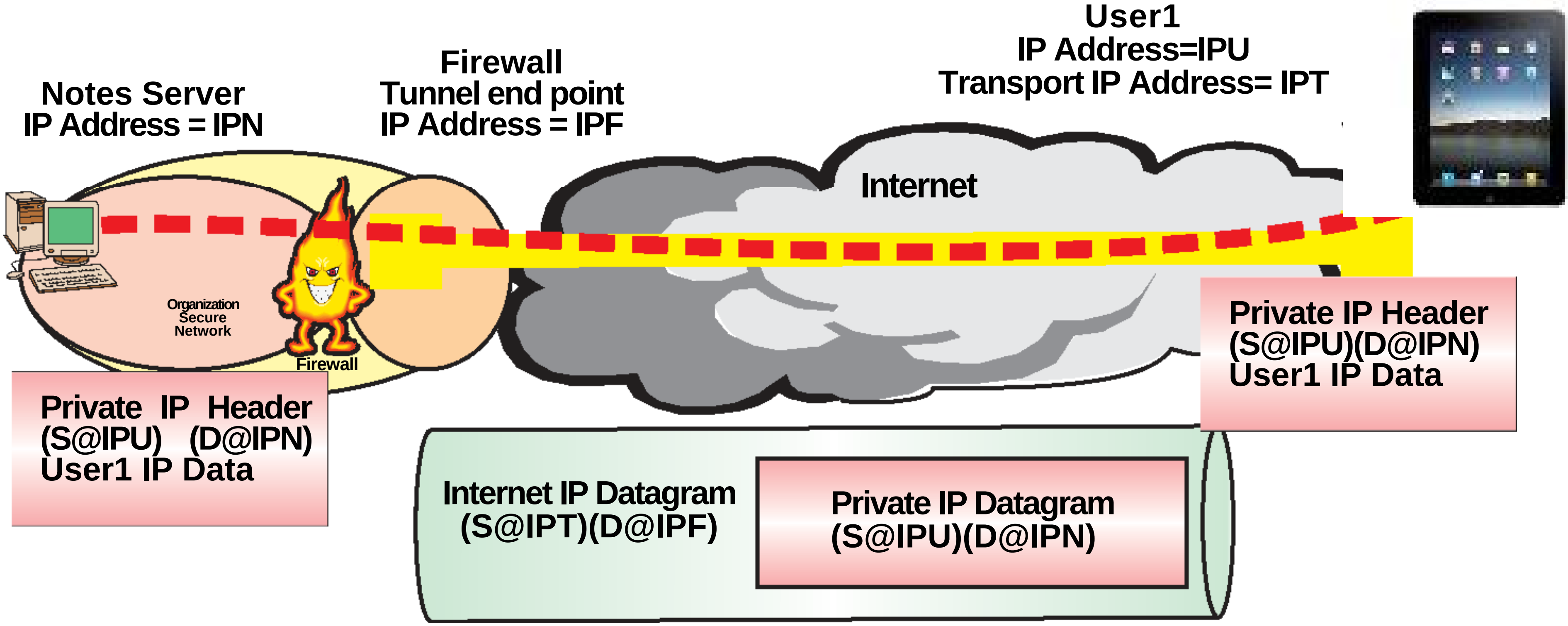
Summary

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



Notes Server
IP Address = IPN

Firewall
Tunnel end point
IP Address = IPF

User1
IP Address=IPU
Transport IP Address= IPT

Private IP Header
(S@IPU) (D@IPN)
User1 IP Data

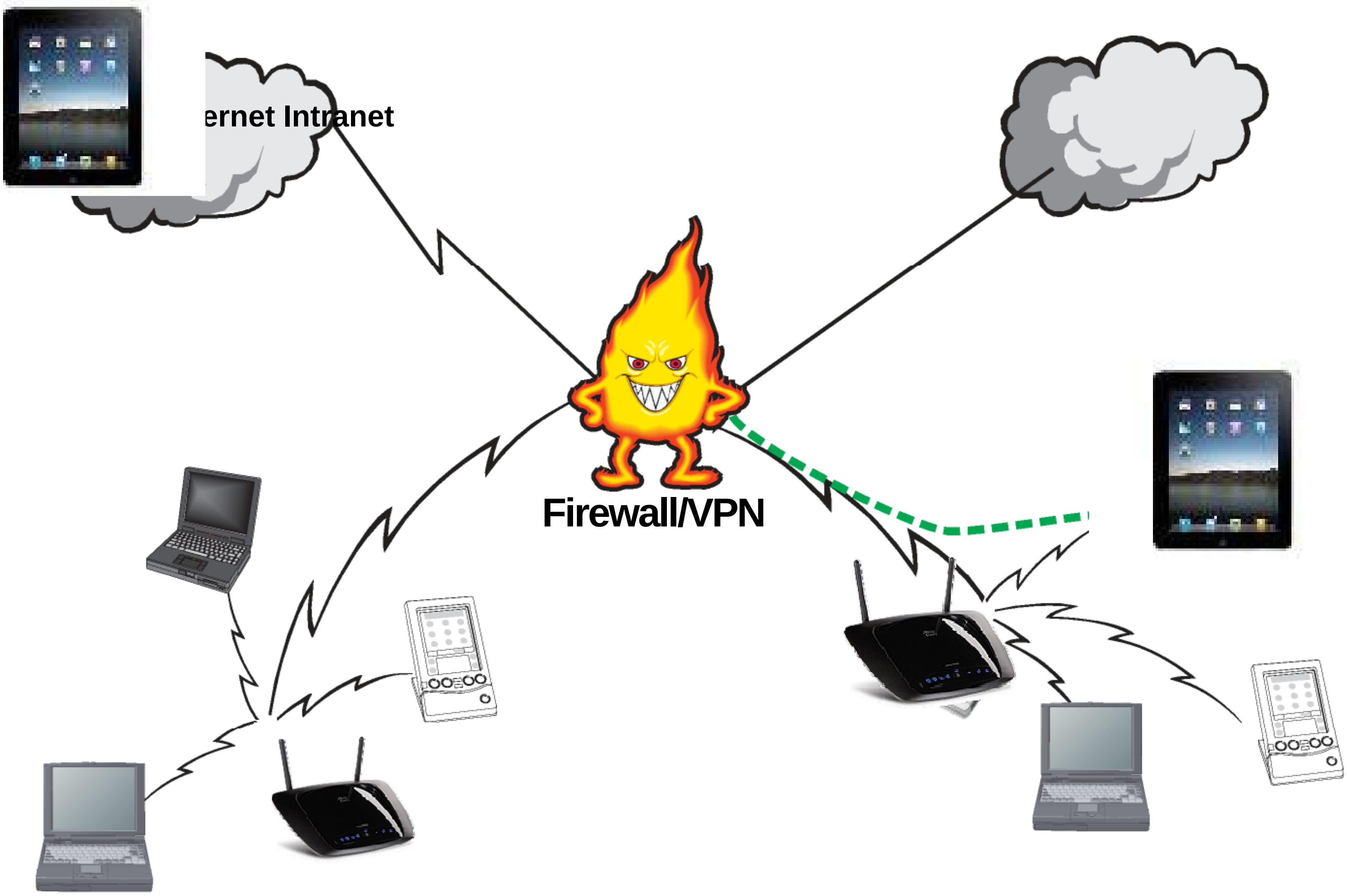
Internet IP Datagram
(S@IPT)(D@IPF)

Private IP Datagram
(S@IPU)(D@IPN)

Private IP Header
(S@IPU)(D@IPN)
User1 IP Data

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

7 bytes	1 byte	6 bytes	6 bytes	4 bytes	2 bytes	Var	Var	4 byte
Preamble	SD	DA	SA	802.1 P/Q	Len	Inf	Pad	FCS

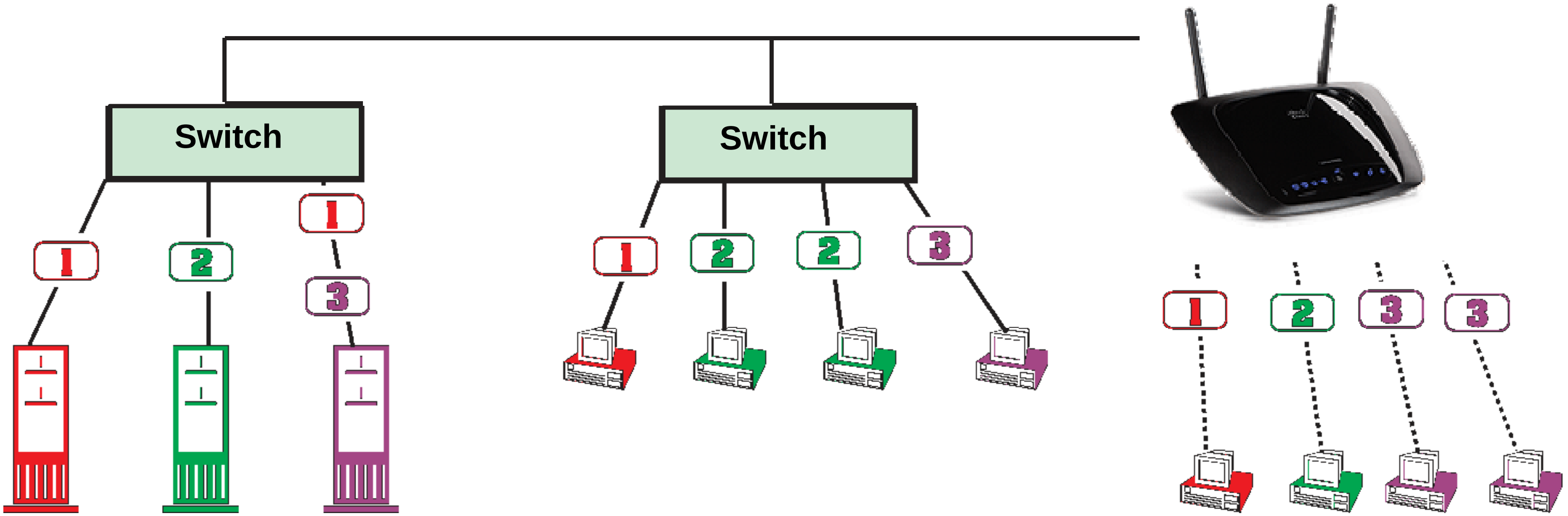
802.1Q header

TPI : Tag protocol identifier
VI : VLAN identifier

802.1P header

P : Priority
C : Canonical format indicator

Anatomy of a VLAN



Manages broadcast domains

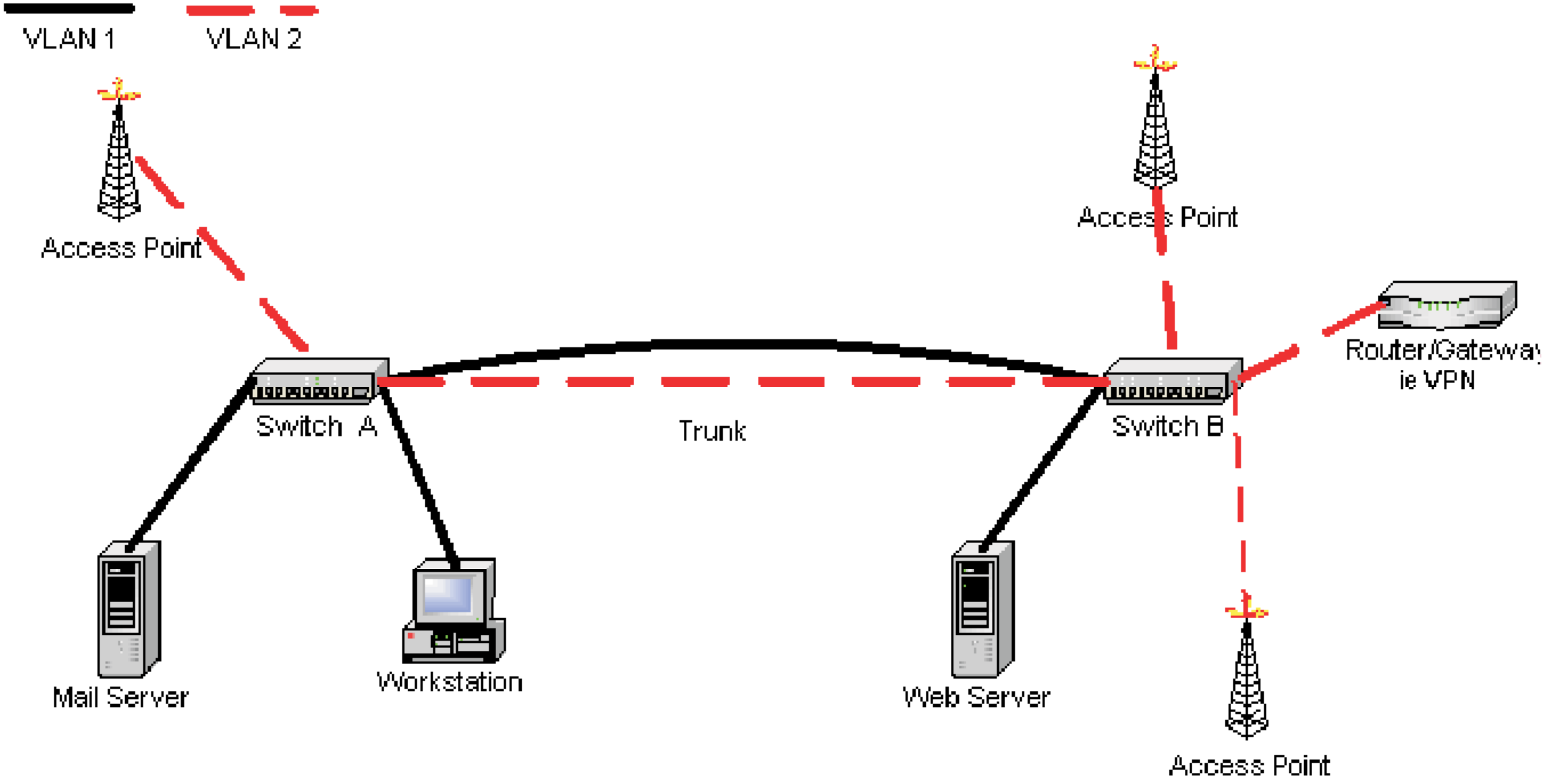
Users and access ports are uniquely assigned to a VLAN

Physical location no longer determines LAN association

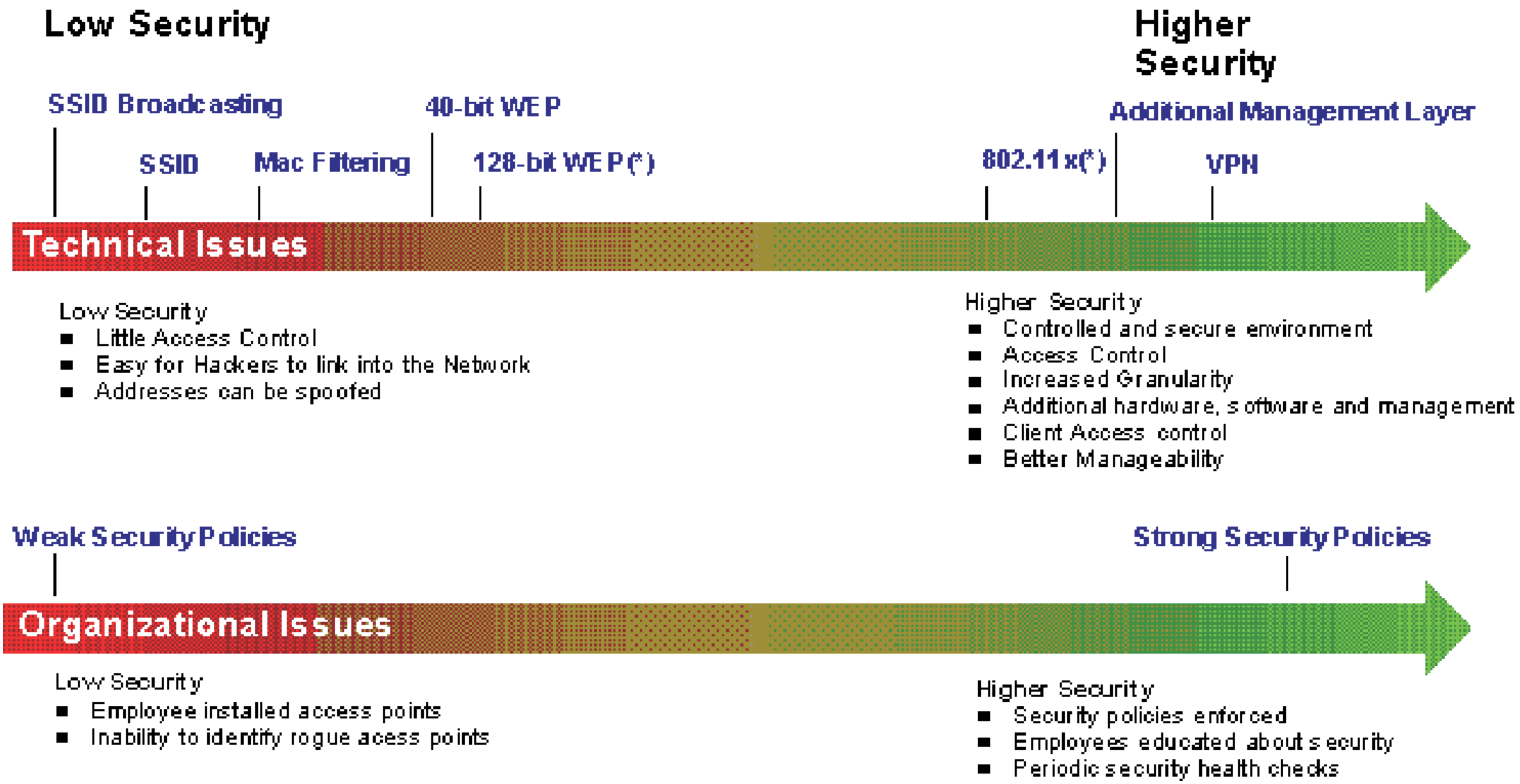
Need to balance benefits with administration requirements

Scalable (but adminstratively rich)

VLANs and WLAN



Wireless Security Review



Low Security

Higher Security

SSID Broadcasting

SSID

Mac Filtering

40-bit WEP

128-bit WEP(*)

802.11x(*)

Additional Management Layer

VPN

Technical Issues

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

Weak Security Policies

Strong Security Policies

Organizational Issues

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

•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

•Choose random subnet address (not the default)

•Use the highest level of WEP/WPA/WPA2

•Firewall your wireless network segment

•Connect the Access Point to the rest of the network with a switch

•Encrypt your wireless traffic using a VPN , TLS, HTTPS ssh……

•Test your wireless security using tools regularly

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

WIKIPEDIA

- WPA - http://en.wikipedia.org/wiki/Wi-Fi_Protected_Access
- WEP - http://en.wikipedia.org/wiki/Wired_Equivalent_Privacy
- 802.1x - http://en.wikipedia.org/wiki/802.1x

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

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)

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)

Questions?

QUESTIONS?

laurak@aesclever.com
www.aesclever.com
650-617-2400
Our other presentations:

Monday, 3:00 am - 4:00 am: Introduction to TCP/IP
Tuesday, 11:00 am – 12:00 pm: What every network manager needs to know about security
Tuesday 1:30 pm – 2:30 pm: Diagnosing Mainframe Network Problems with Packet Trace
Wednesday 11:00 am – 12:00 pm: Cloud Computing Environment
Wednesday 1:30 pm – 2:30 pm: Hot Topics in Networking and Security
Wednesday 4:30 pm – 5:30 pm: Wireless Security Challenges
Thursday 11:00 am – 12:00 pm: Virtualization – The Evolution of the Data Center