# Wireless Switching Arquitetura Centralizada e Segurança de Redes Sem-Fio GTER – 17

Luiz Eduardo Dos Santos
luiz at arubanetworks.com

ARUBA
WIRELESS NETWORKS

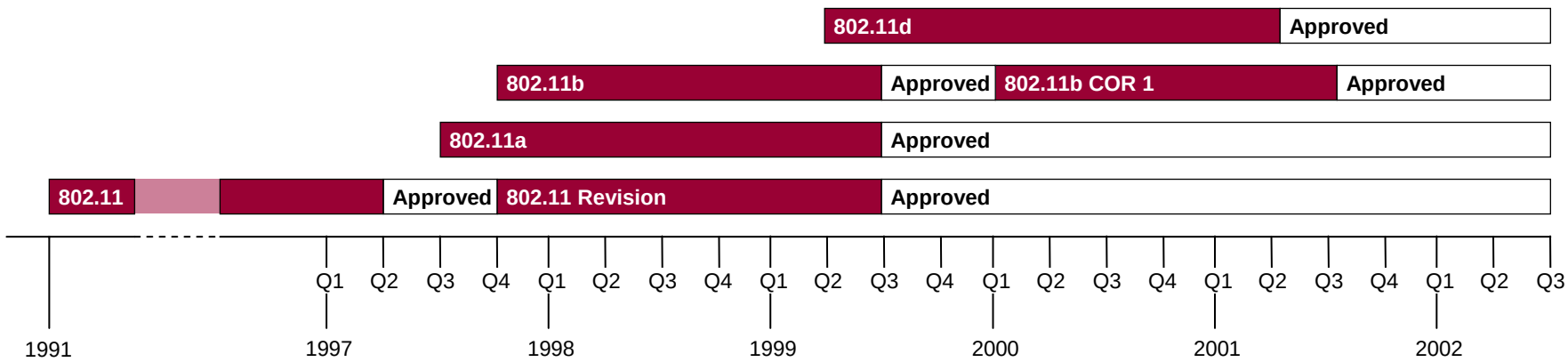
# Agenda

- Brief History
- WiFi Today
- WiFi Switching
- WiFi Switching Benefits
- RF Management
- Mobility
- Security
- Resources



ARUBA WIRELESS NETWORKS

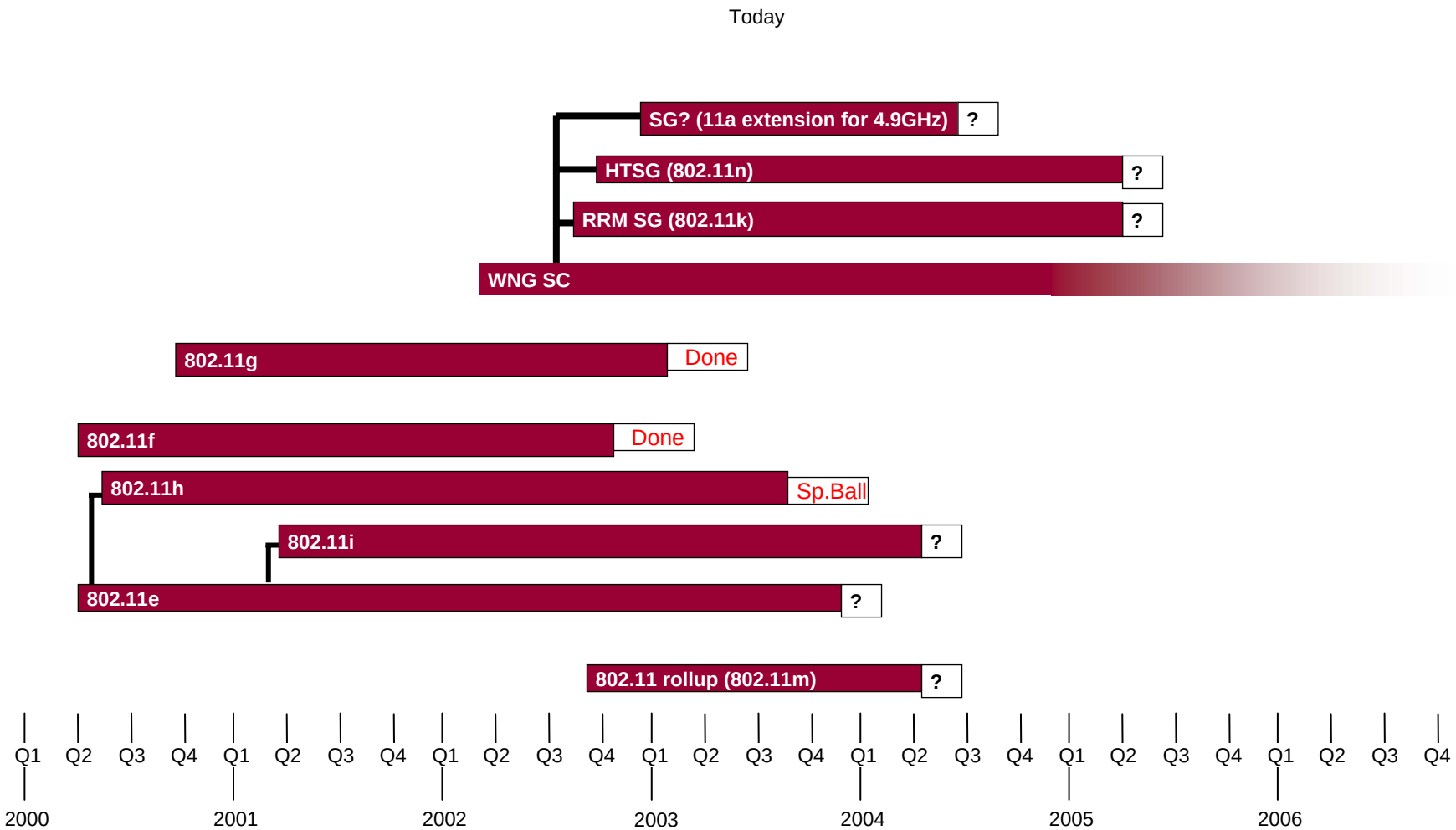
# 802.11 History






ARUBA WIRELESS NETWORKS

# 802.11 Timeline (as of Oct'03)






ARUBA WIRELESS NETWORKS

# WEP Broken

- WEP is vulnerable because of relatively short IVs and keys that remain static.
- possible to compute the bit difference of two CRCs based on the bit difference of the messages
- http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html

# Standards-based Solutions to WEP

- WPA/Pre-Shared Key
- WPA /TKIP & 802.1x + EAP(PEAP, LEAP, TLS, TTLS)
- 802.11i
- VPNs on top of WEP

| Security Requirements | WEP | WPA |
|---|---|---|
| Authentication | broken | EAP, 802.1x |
| Access control | broken | 802.1x |
| Replay prevention | not implemented | TKIP packet counter |
| Message modification detection | broken | Michael |
| Message privacy | broken with 4-5 mill. packets | TKIP |
| Key protection | only master key | broken |

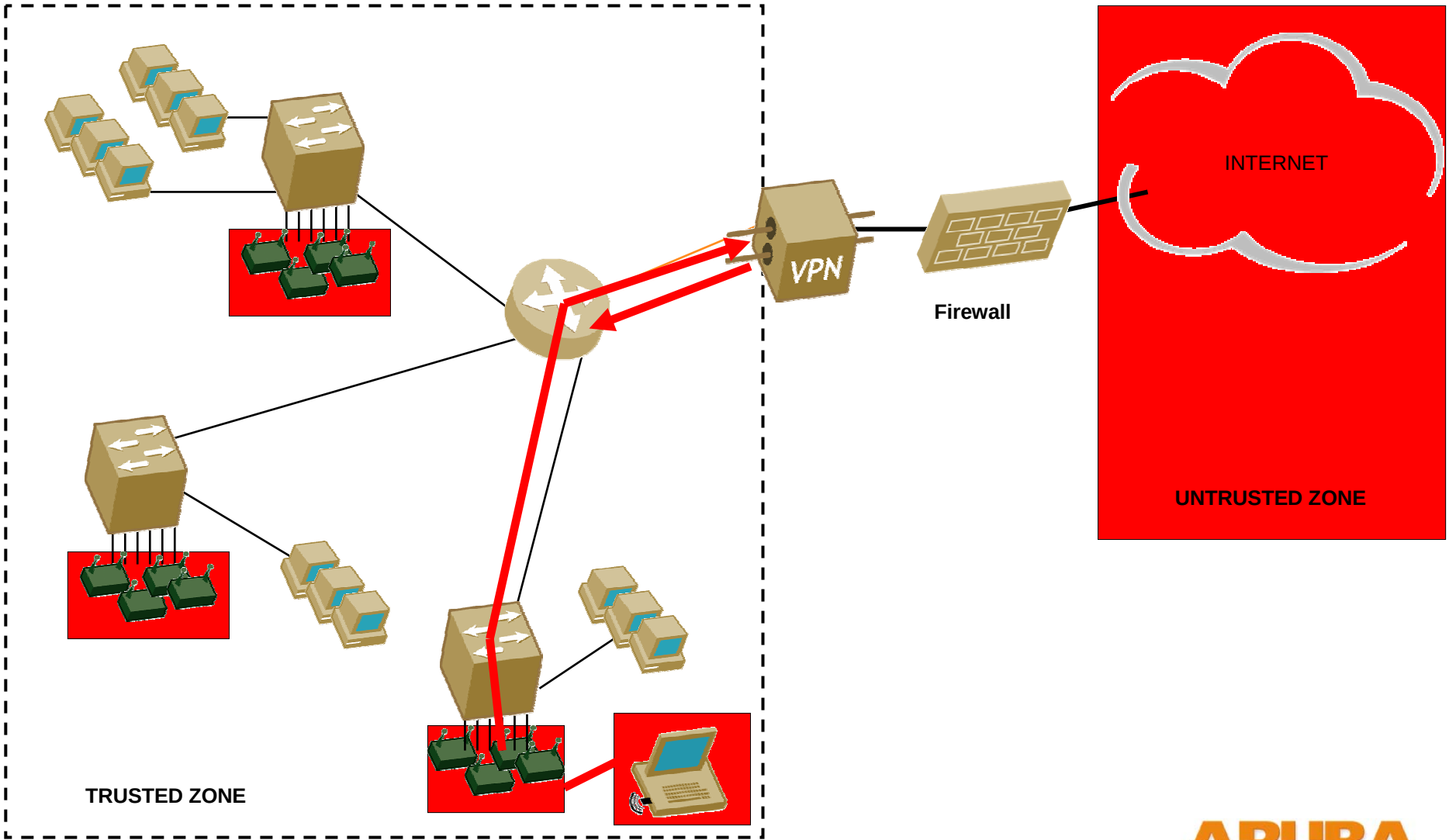


ARUBA WIRELESS NETWORKS

# Agenda

- Brief History
- WiFi Today
- WiFi Switching
- WiFi Switching Benefits
- RF Management
- Mobility
- Security
- Resources

# WiFi in the enterprise





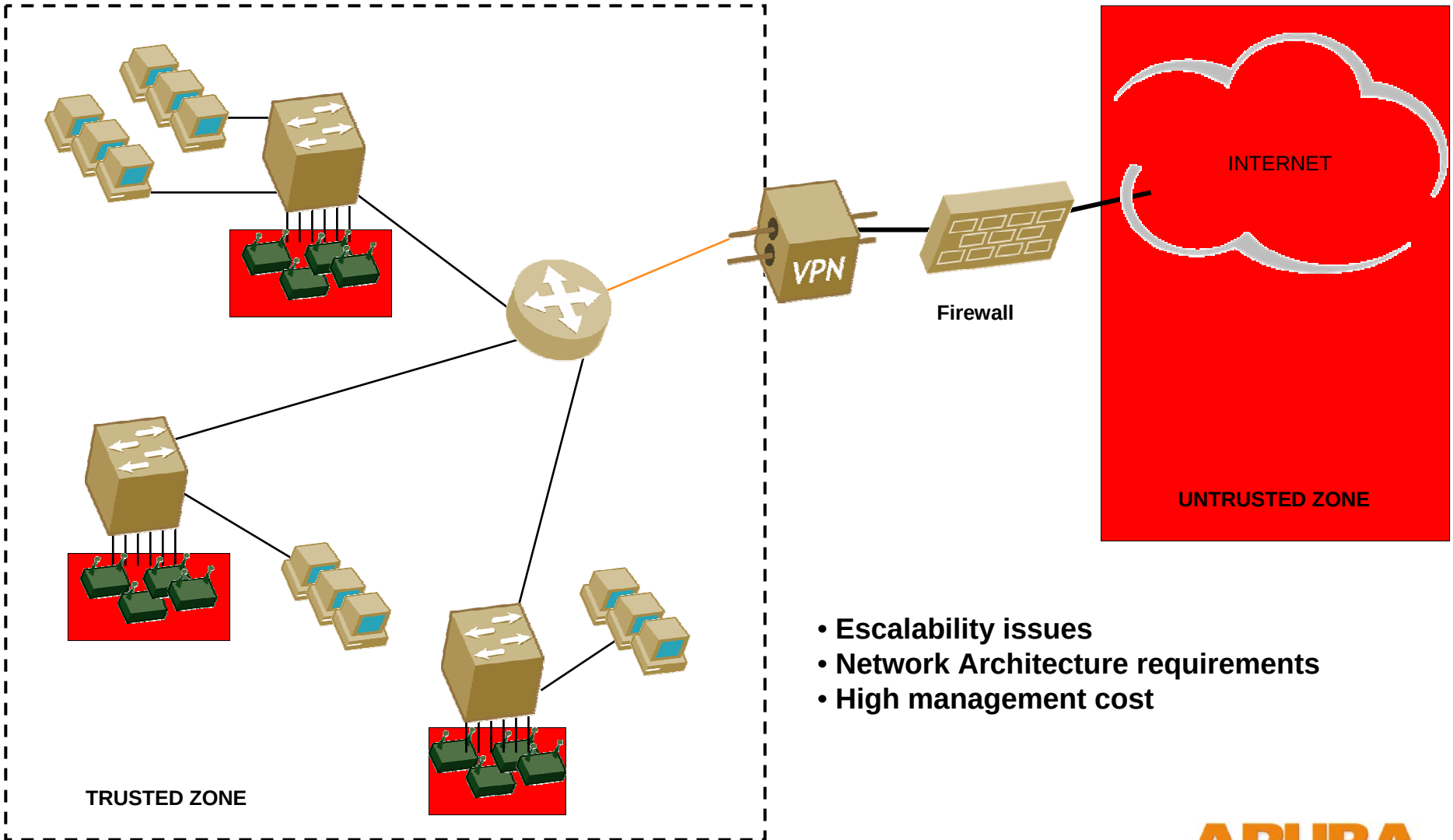

ARUBA WIRELESS NETWORKS

# WiFi in the enterprise



ARUBA WIRELESS NETWORKS

# WiFi in the enterprise




- **Escalability issues**
- **Network Architecture requirements**
- **High management cost**



ARUBA WIRELESS NETWORKS

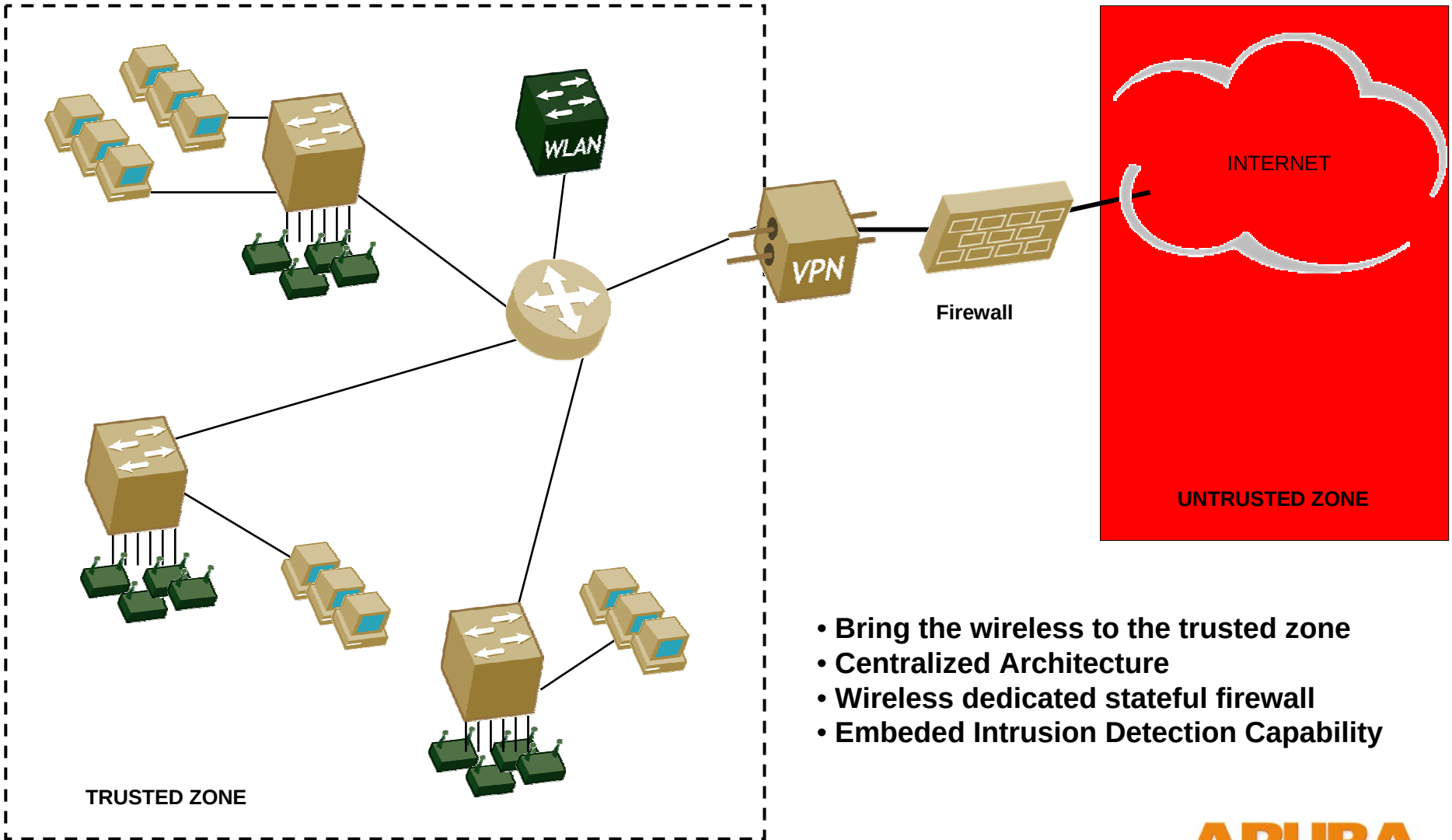
# Agenda

- Brief History
- WiFi Today
- WiFi Switching
- WiFi Switching Benefits
- RF Management
- Mobility
- Security
- Resources



ARUBA WIRELESS NETWORKS

# WiFi Switching



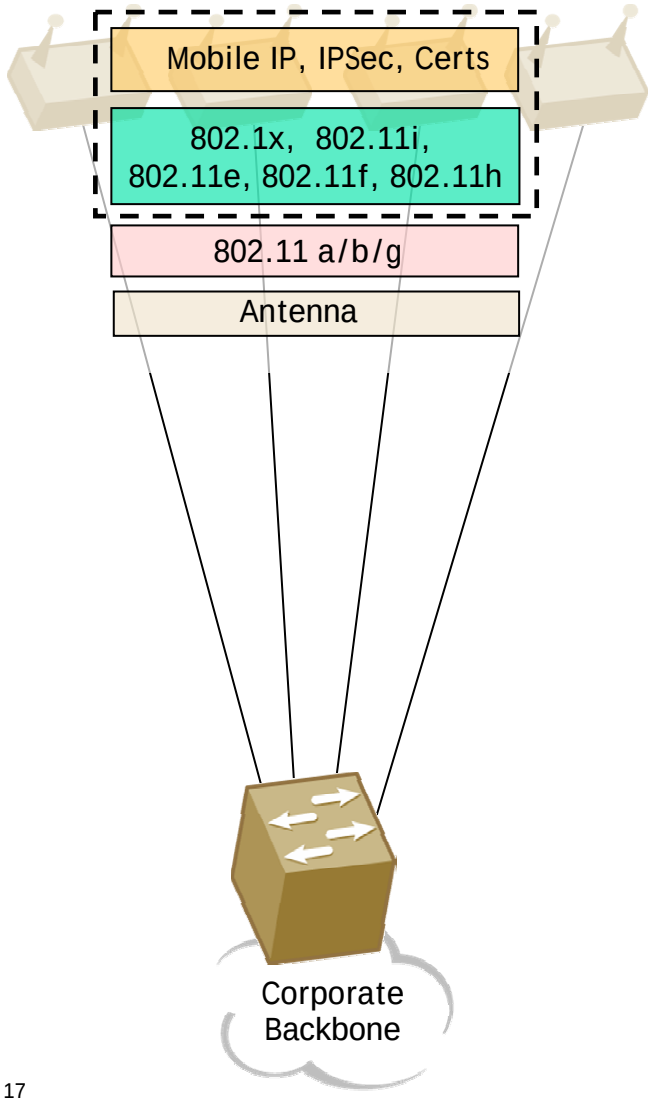

- **Bring the wireless to the trusted zone**
- **Centralized Architecture**
- **Wireless dedicated stateful firewall**
- **Embeded Intrusion Detection Capability**



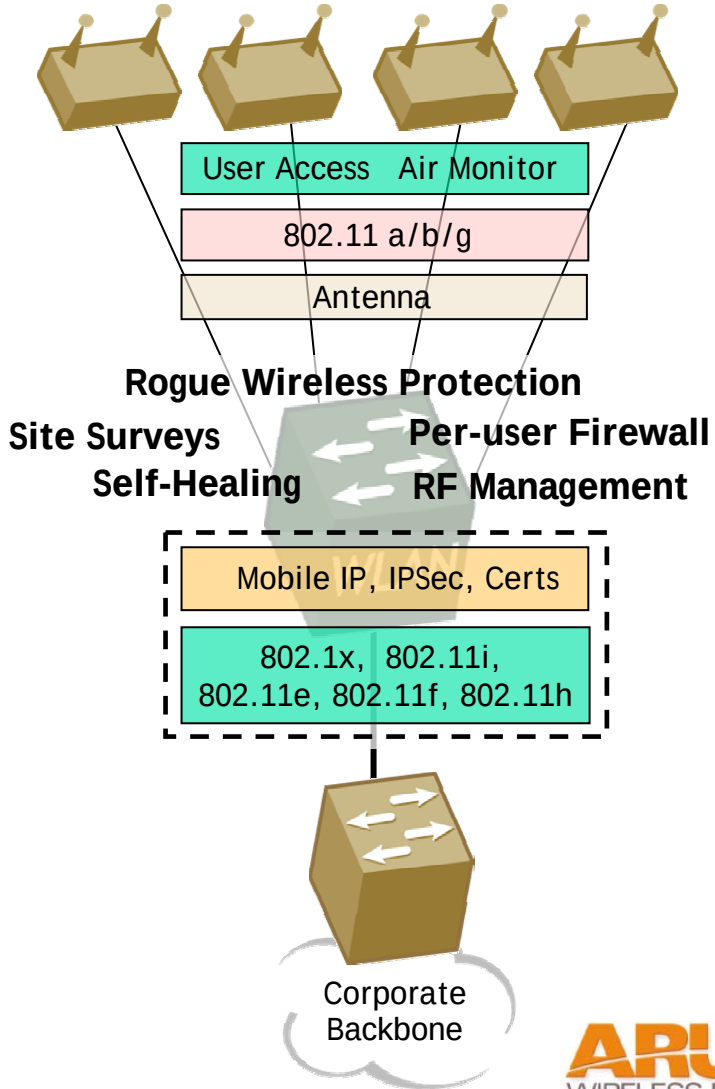
ARUBA WIRELESS NETWORKS

# Splitting the AP

## Decentralized




## Centralized



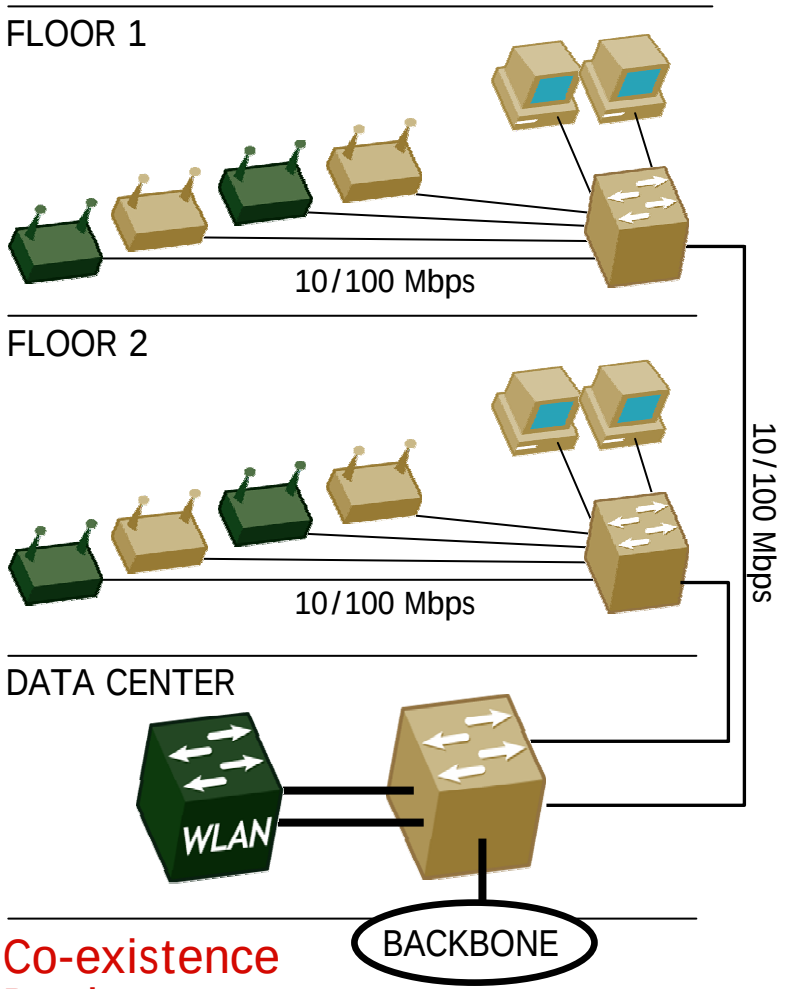



ARUBA WIRELESS NETWORKS

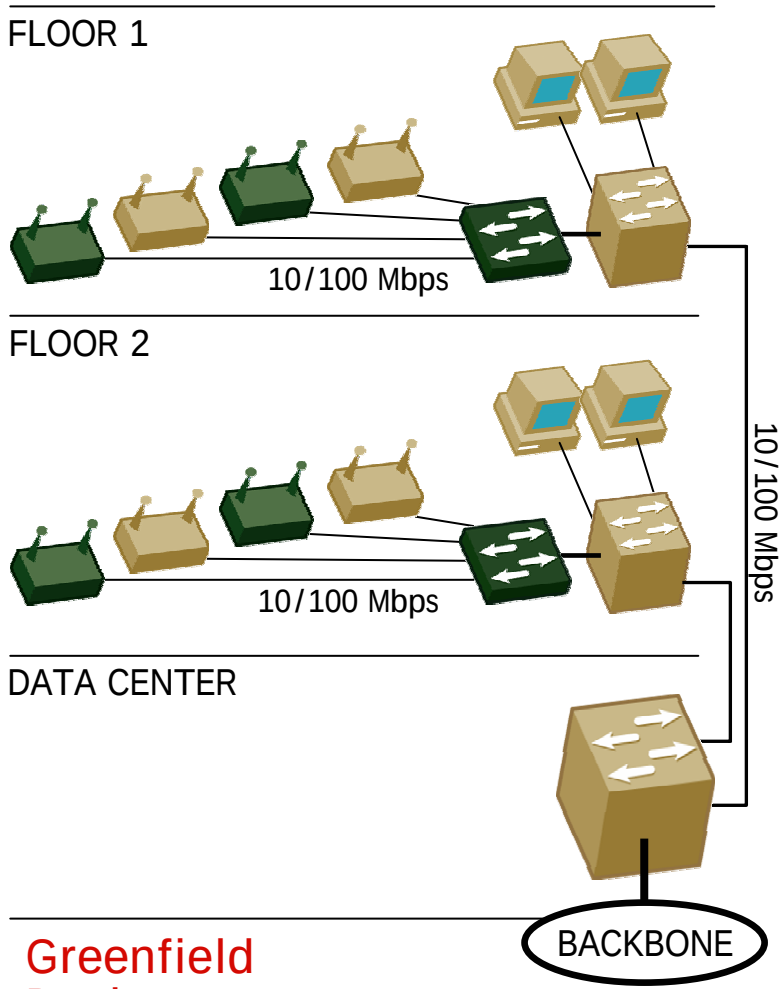
# Agenda

- Brief History
- WiFi Today
- What is WiFi Switching?
- WiFi Switching Benefits
- RF Management
- Mobility
- Security
- Resources

# “Drop-in” Co-existence




Co-existence Deployment

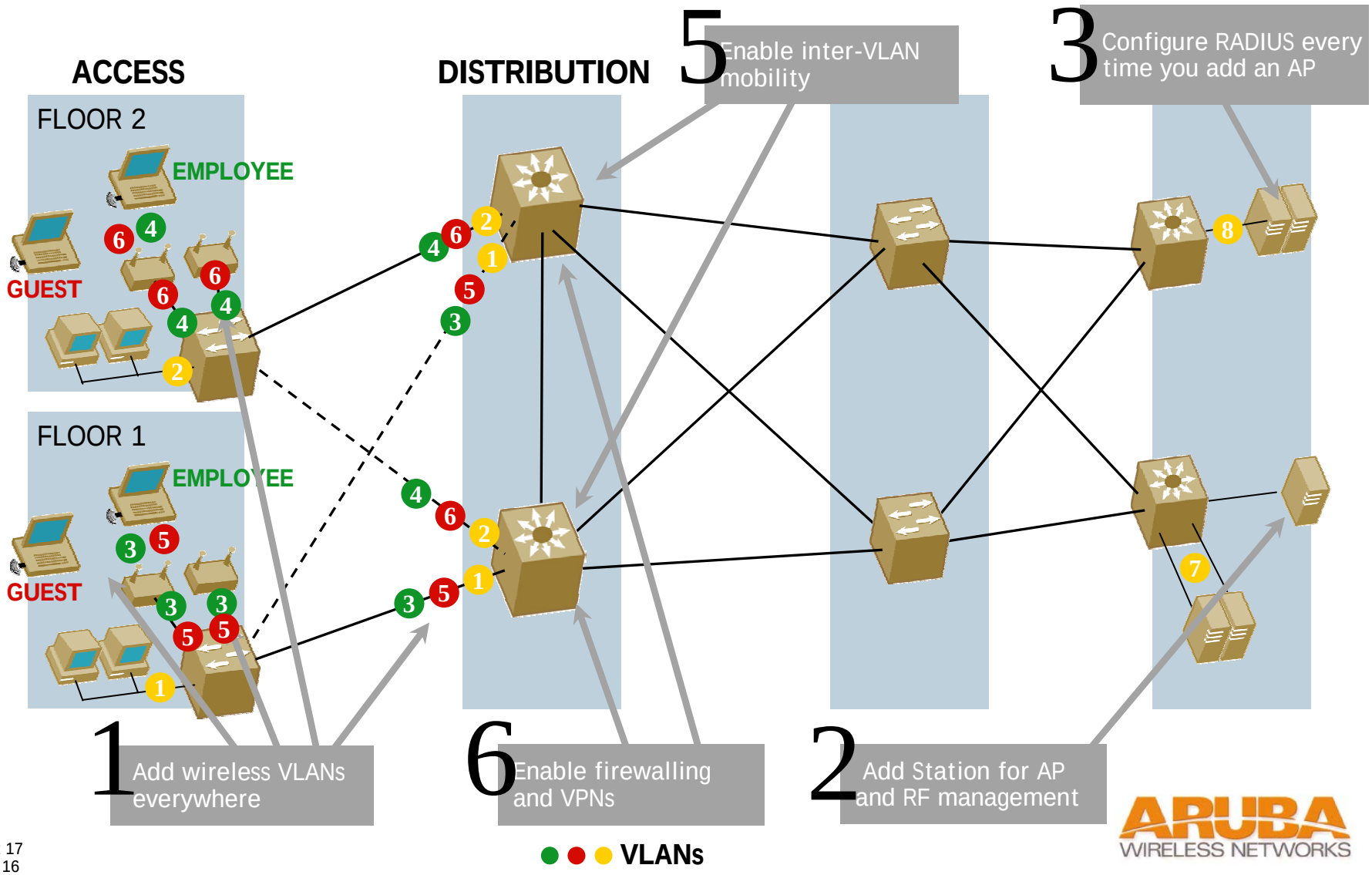



Greenfield Deployment



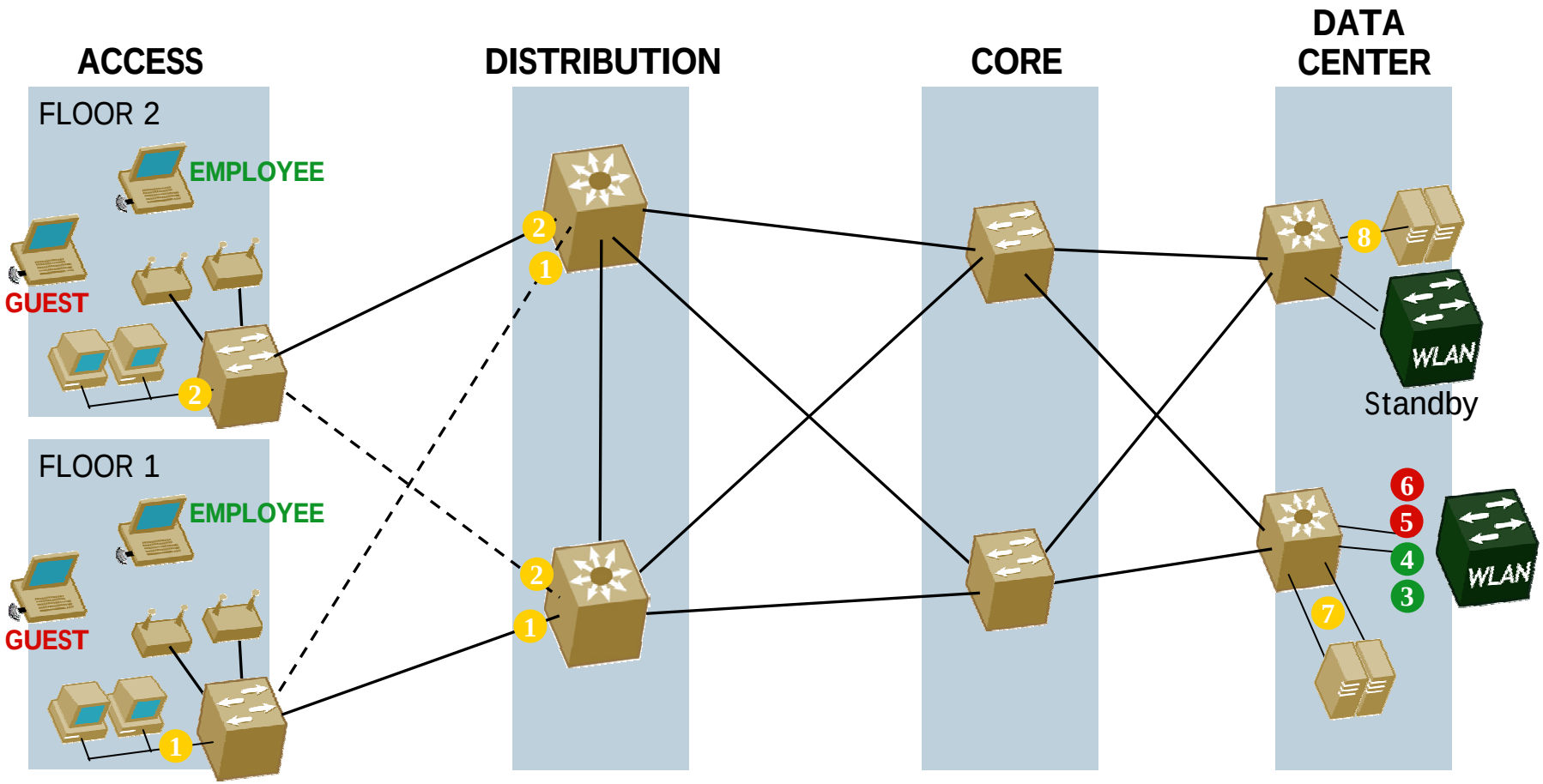
ARUBA WIRELESS NETWORKS

# Decentralized Model



# Centralized Model

## Simplified and Scalable with Wi-Fi Switching



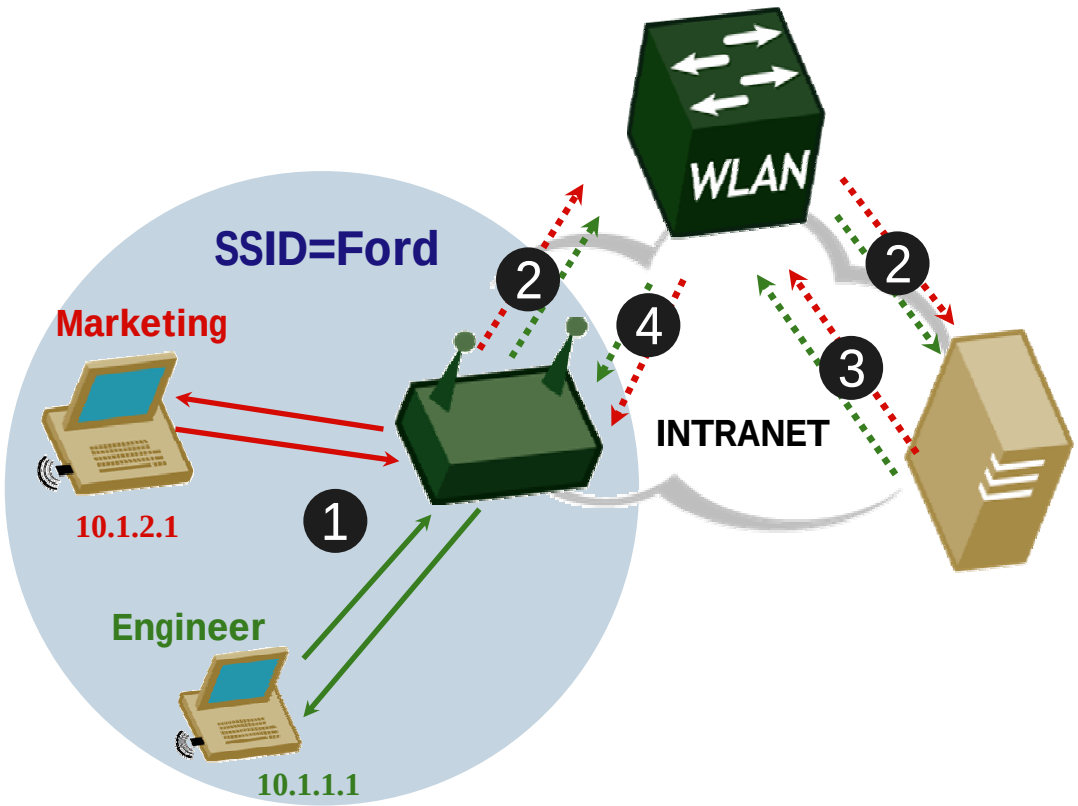



● ● ● VLANs

ARUBA WIRELESS NETWORKS

# Role-Based VLANs

## For Logical Traffic Separation on the Wire



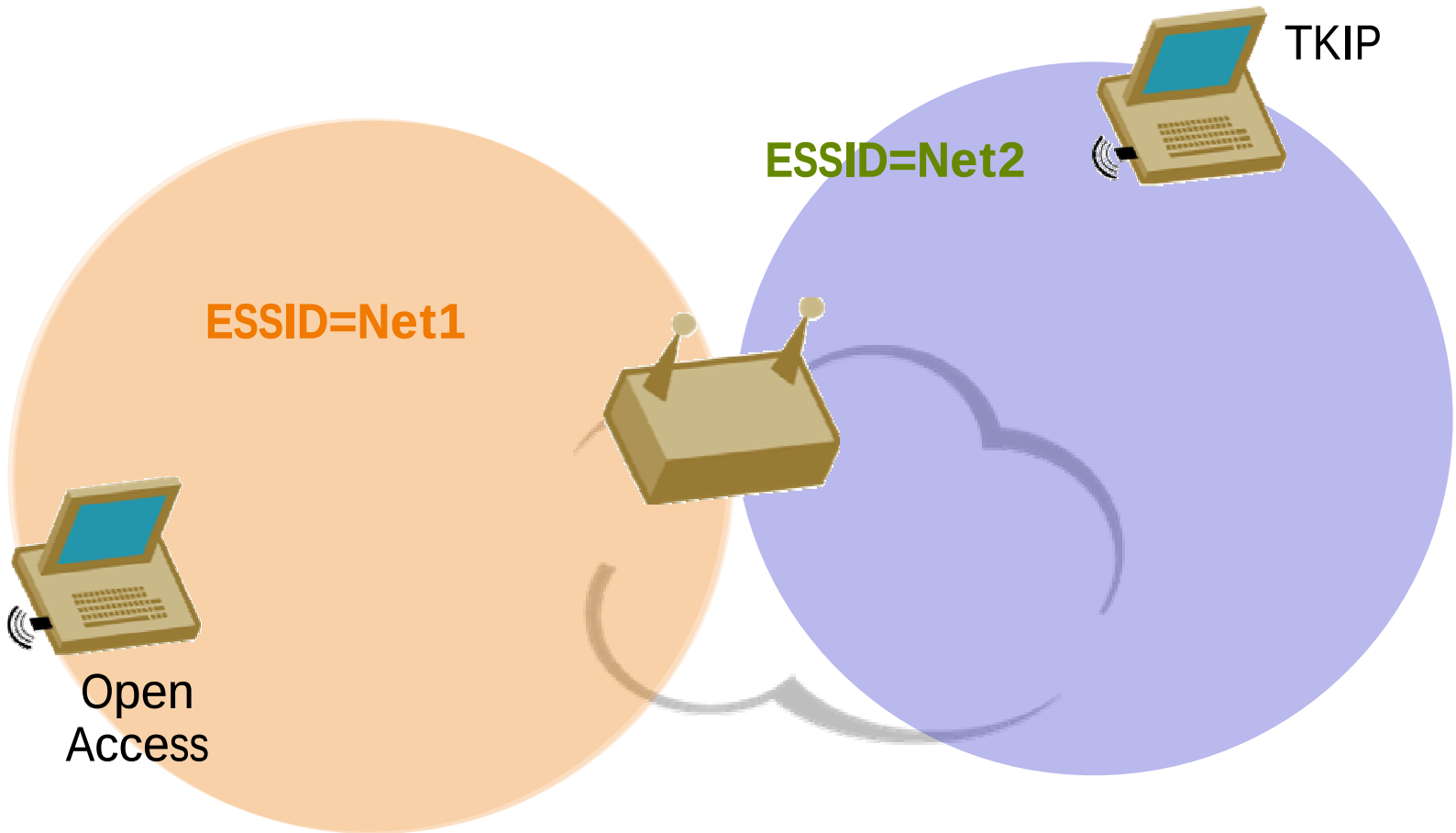

1. Each station associates with a single corporate SSID.
2. Authorization (802.1X) request is forwarded to RADIUS
3. RADIUS responds with authorization response and VLAN identifier
4. WLAN switch parses RADIUS response and automatically assigns station to the correct VLAN



ARUBA WIRELESS NETWORKS

# Virtual AP

Enables “Crypto-VLANs”

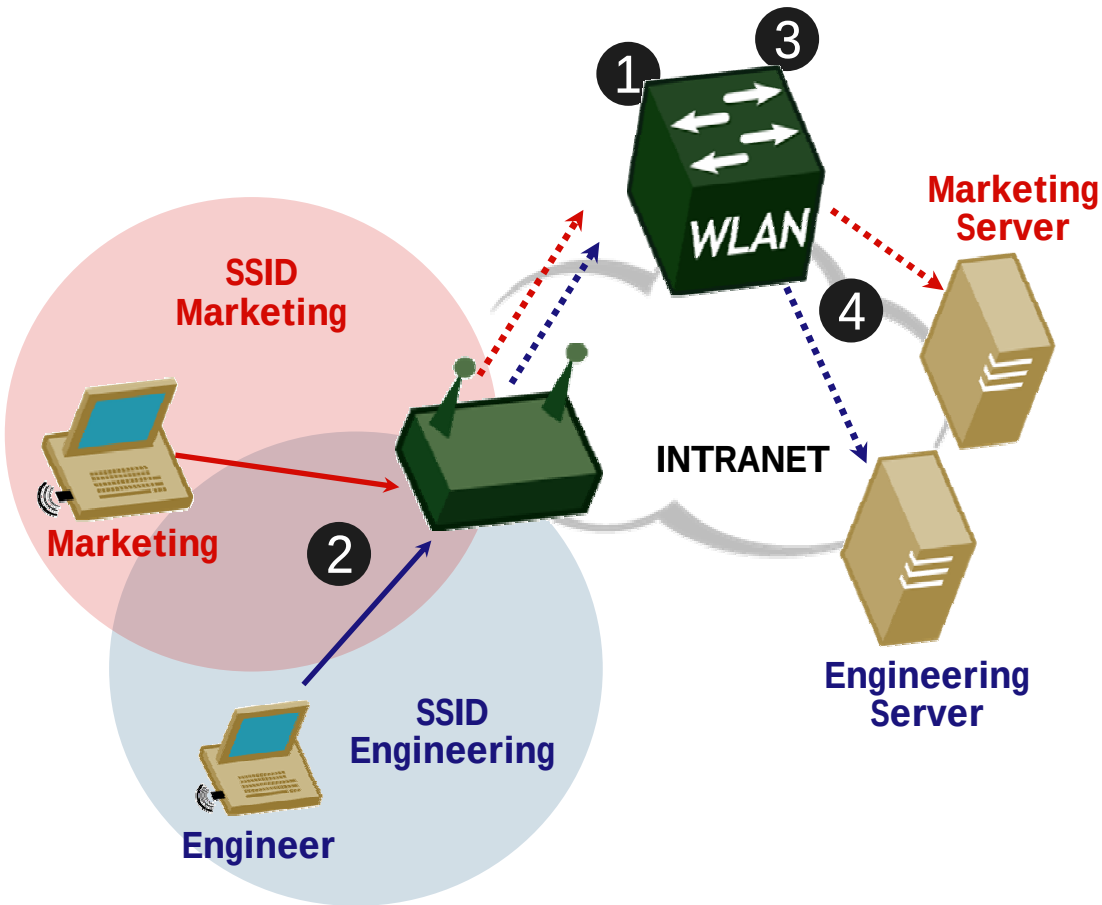





ARUBA WIRELESS NETWORKS

# ESSID-Based VLANs

## For Physical Traffic Separation in the Air



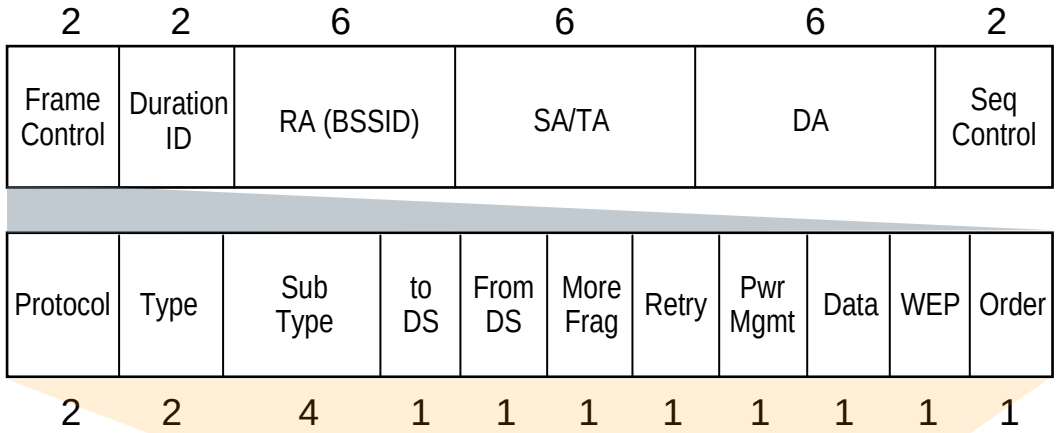

1. ESSID-to-VLAN pairing is pre-configured in the WLAN switch
2. Stations associate to the AP with the appropriate ESSID
3. WLAN assigns the correct VLAN to the respective stations based on ESSID-to-VLAN configuration
4. Data traffic is forward to the appropriate VLAN by the WLAN switch



ARUBA WIRELESS NETWORKS

# Real Wi-Fi Switch advantage?

**802.11 Frame**




Processing native .11 frames brings access to valuable wireless-specific information that traditional Ethernet switches don't

- Advanced load balancing based on signal quality
- Low latency inter-switch handoff
- No VLAN explosion at APs
- Frames Encrypted through the intranet
- Advanced troubleshooting
- Detection and protection against wireless attacks
- Control multicast to APs only when there's an associated station



ARUBA WIRELESS NETWORKS

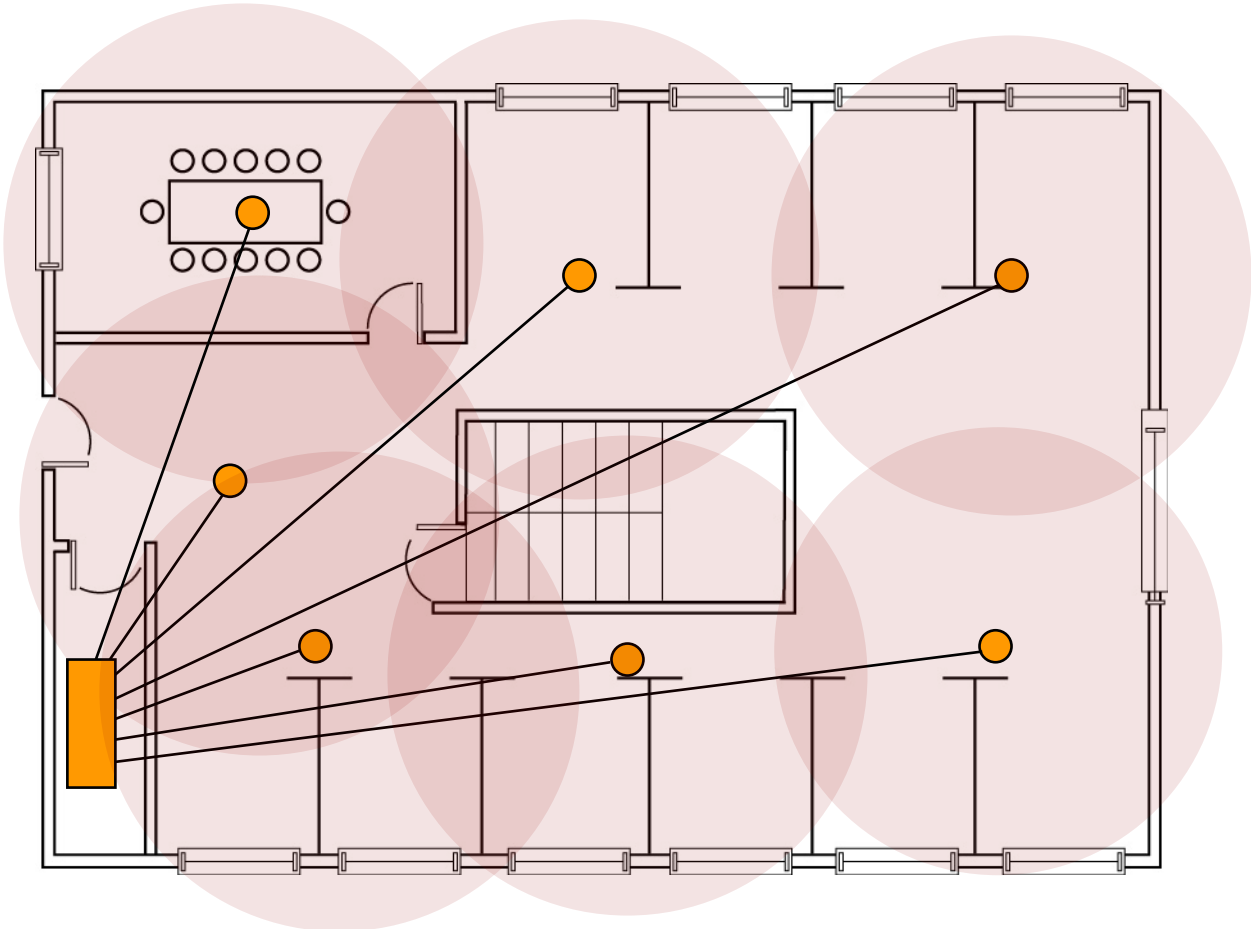
# Agenda

- Brief History
- WiFi Today
- WiFi Switching
- WiFi Switching Benefits
- RF Management
- Mobility
- Security
- Resources



ARUBA WIRELESS NETWORKS

# Self-Calibrating Wi-Fi

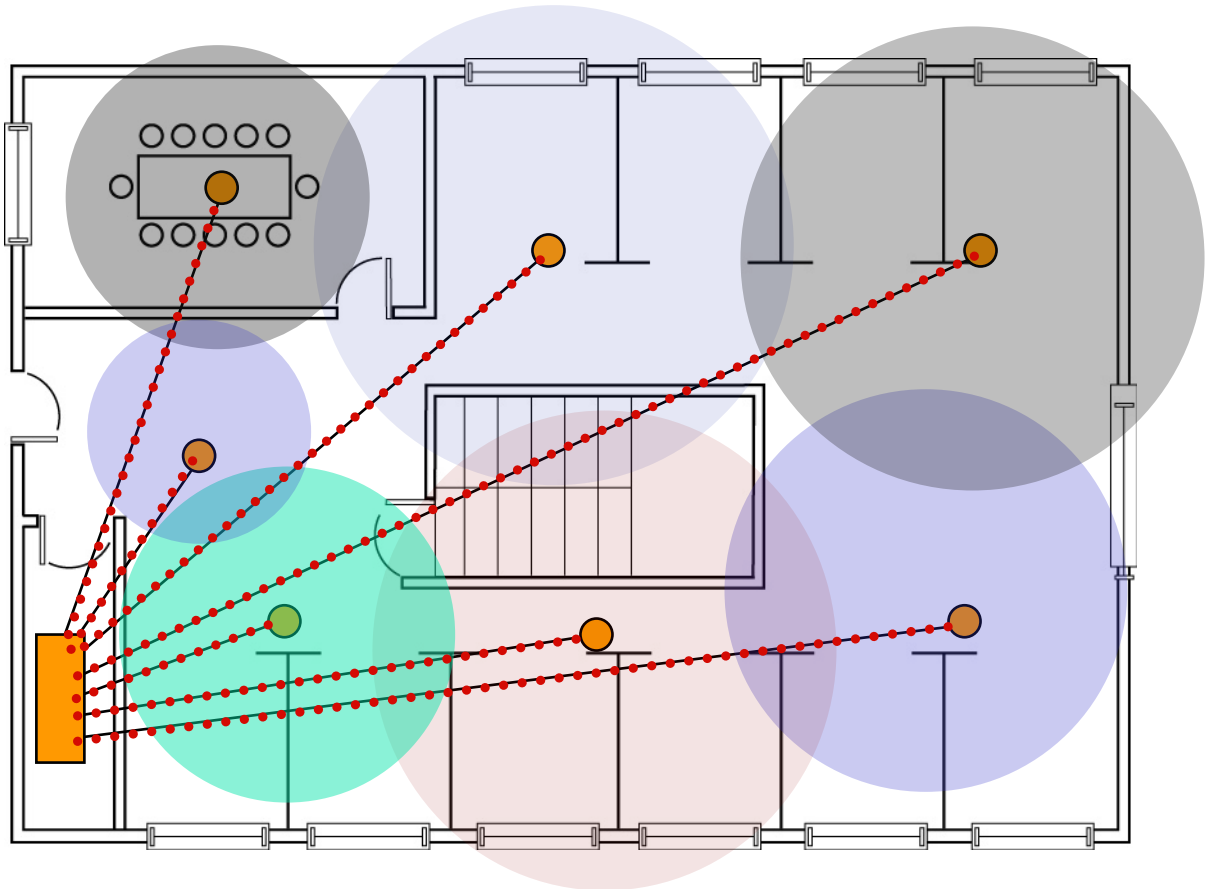


Real-time calibration characterizes the indoor propagation to determine the actual channel and transmit power settings of each AP



ARUBA WIRELESS NETWORKS

# Self-Calibrating Wi-Fi

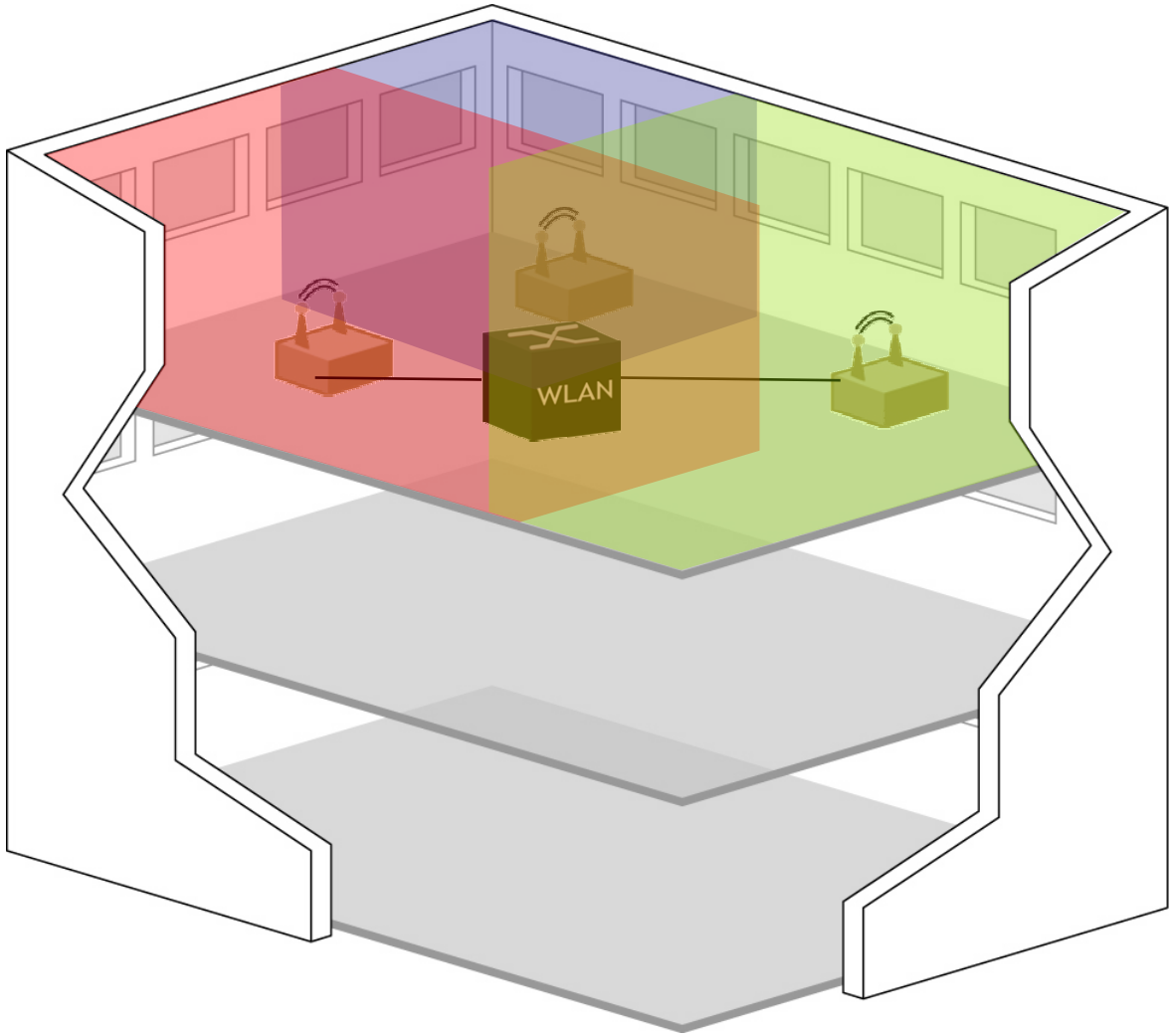


Real-time calibration characterizes the indoor propagation to determine the actual channel and transmit power settings of each AP



ARUBA WIRELESS NETWORKS

# Self-Healing Wi-Fi




- WLAN switch automatically reconfigures AP to extend coverage to compensate
- Plug and Play APs download original config



ARUBA WIRELESS NETWORKS

# Agenda

- Brief History
- WiFi Today
- WiFi Switching
- WiFi Switching Benefits
- RF Management
- Mobility
- Security
- Resources



ARUBA WIRELESS NETWORKS

# Mobility is All About the User

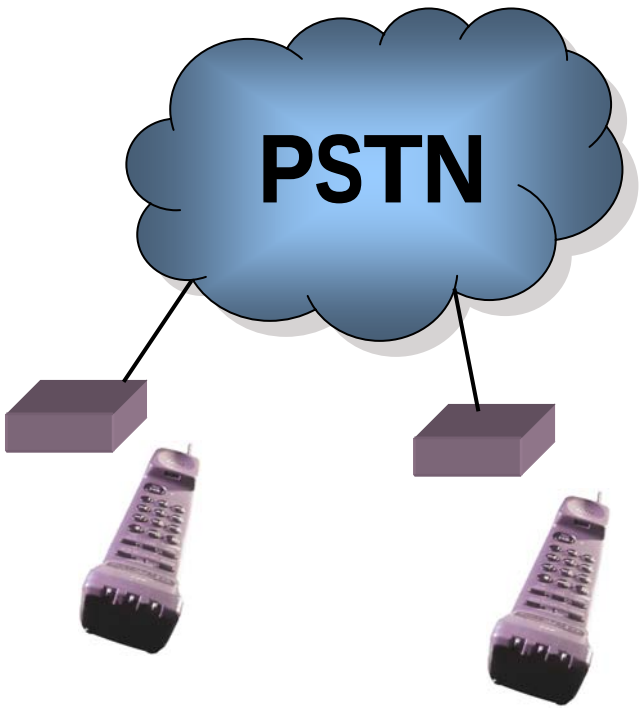
| USER IDENTITY | USER LOCATION | USER PRESENCE |
| --- | --- | --- |
|  |  |  |
| Who the user is | Where the user is | If the user is available |

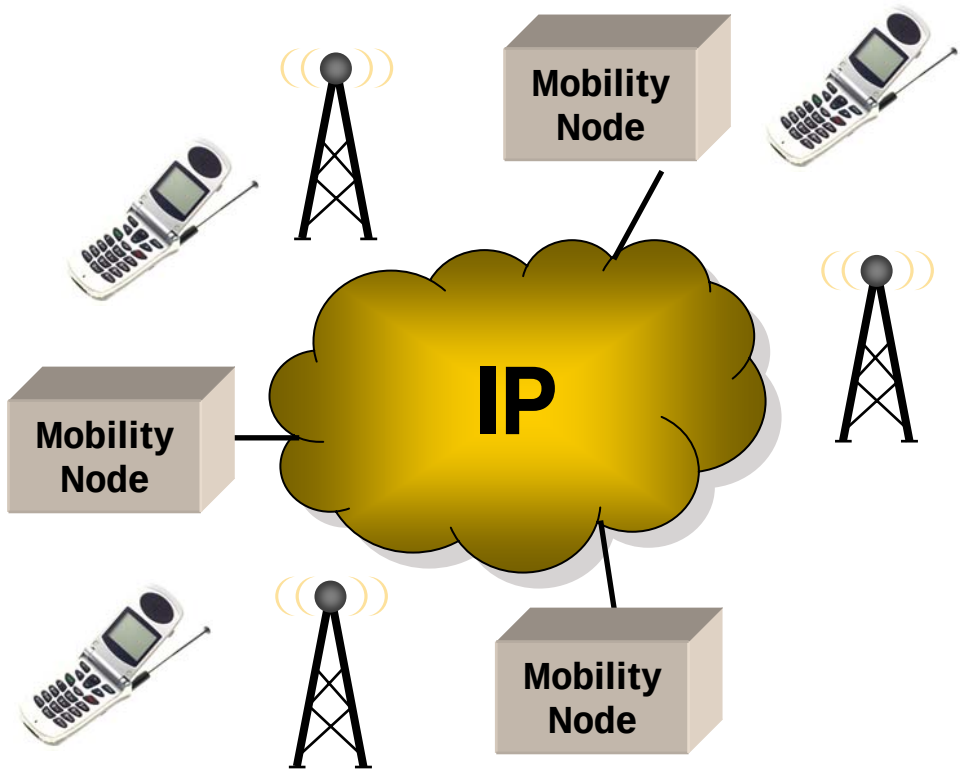



ARUBA WIRELESS NETWORKS

# Purpose-Built Architecture for Cellular

- Hierarchy is important to scale
- Functional separation is key to keep pace with change

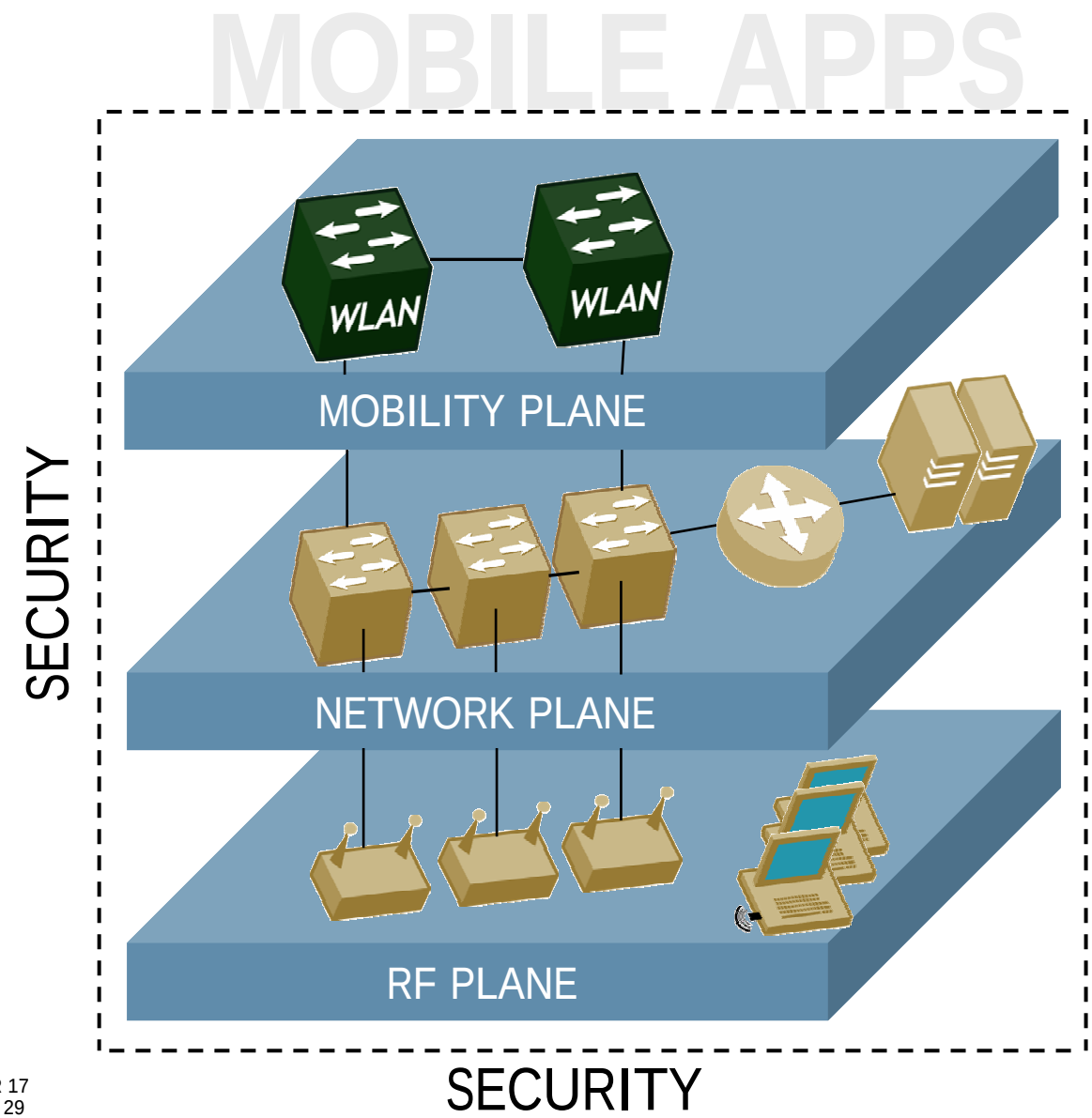





ARUBA WIRELESS NETWORKS

# A New Architecture for Mobility

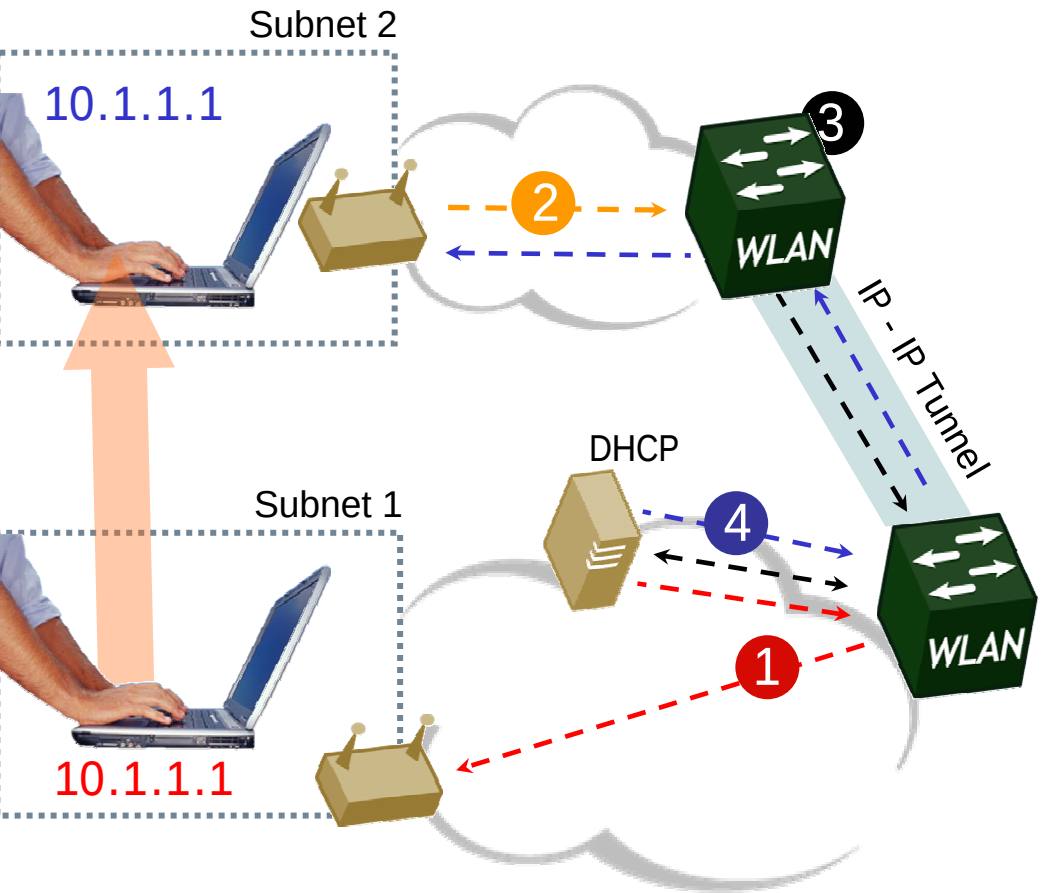



- Integrate or overlay?



ARUBA WIRELESS NETWORKS

# Seamless Mobility

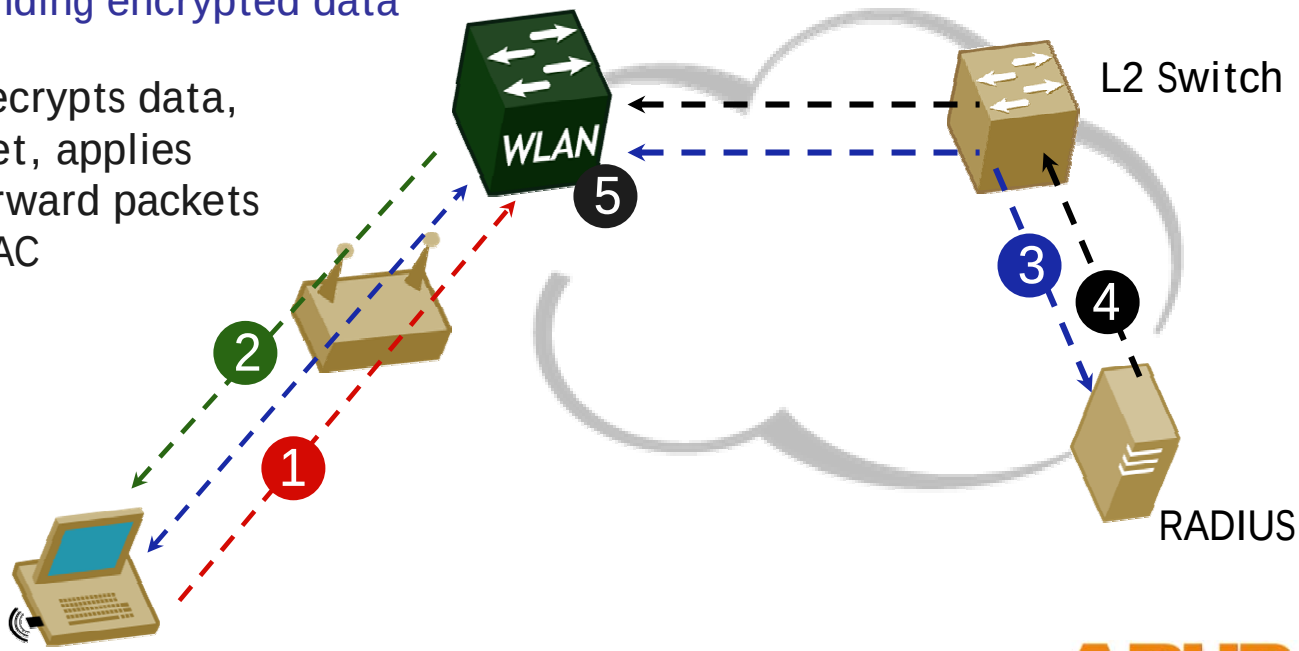



1. Client receives initial IP address from DHCP server based on his VLAN association
2. Client moves to new subnet and issues another DHCP request
3. Using proxy DHCP, the Wi-Fi switch modifies request with same initial IP address
4. Client receives same IP address on different subnet
5. Intelligent client mobility integrated into the switch ensures seamless connectivity as users move between switches

ARUBA WIRELESS NETWORKS

# Centralized 802.1x Authentication

1. Client sends 802.11 association request that is automatically forwarded by AP to WLAN switch
2. WLAN switch responds with association acknowledgement
3. Client and WLAN switch start 802.1x authentication conversation along with RADIUS server
4. Encryption keys pass to the WLAN switch and user derives own encryption keys…begins sending encrypted data
5. WLAN switch decrypts data, processes packet, applies services and forward packets based on .11 MAC



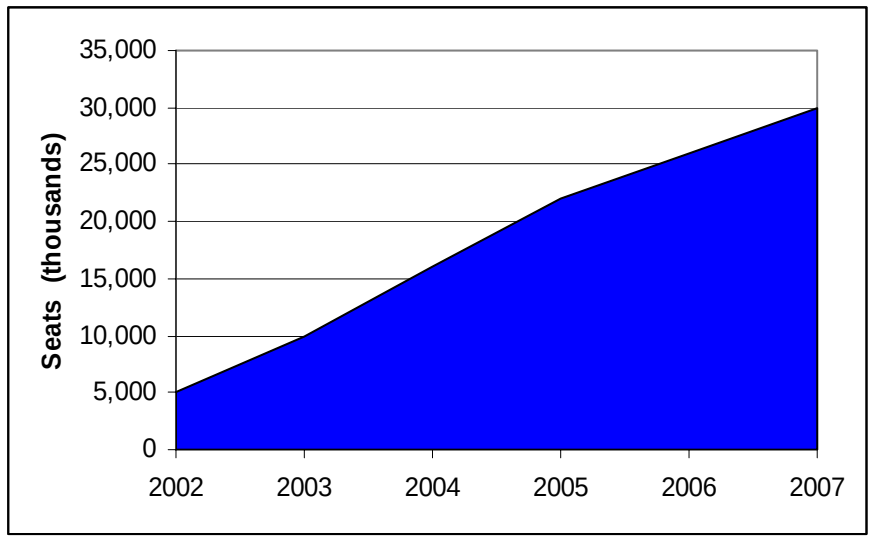



ARUBA WIRELESS NETWORKS

# Why Voice Over Wireless?

- Cost savings from running intra-campus calls over cellular
- ROI on unified voice/data network
- Multi-mode (GSM, Wi-Fi) phones emerging
- Explosion of VoIP gear


**Worldwide IP-PBX Premise Equipment Shipments**




*Source: Allied Business Intelligence*

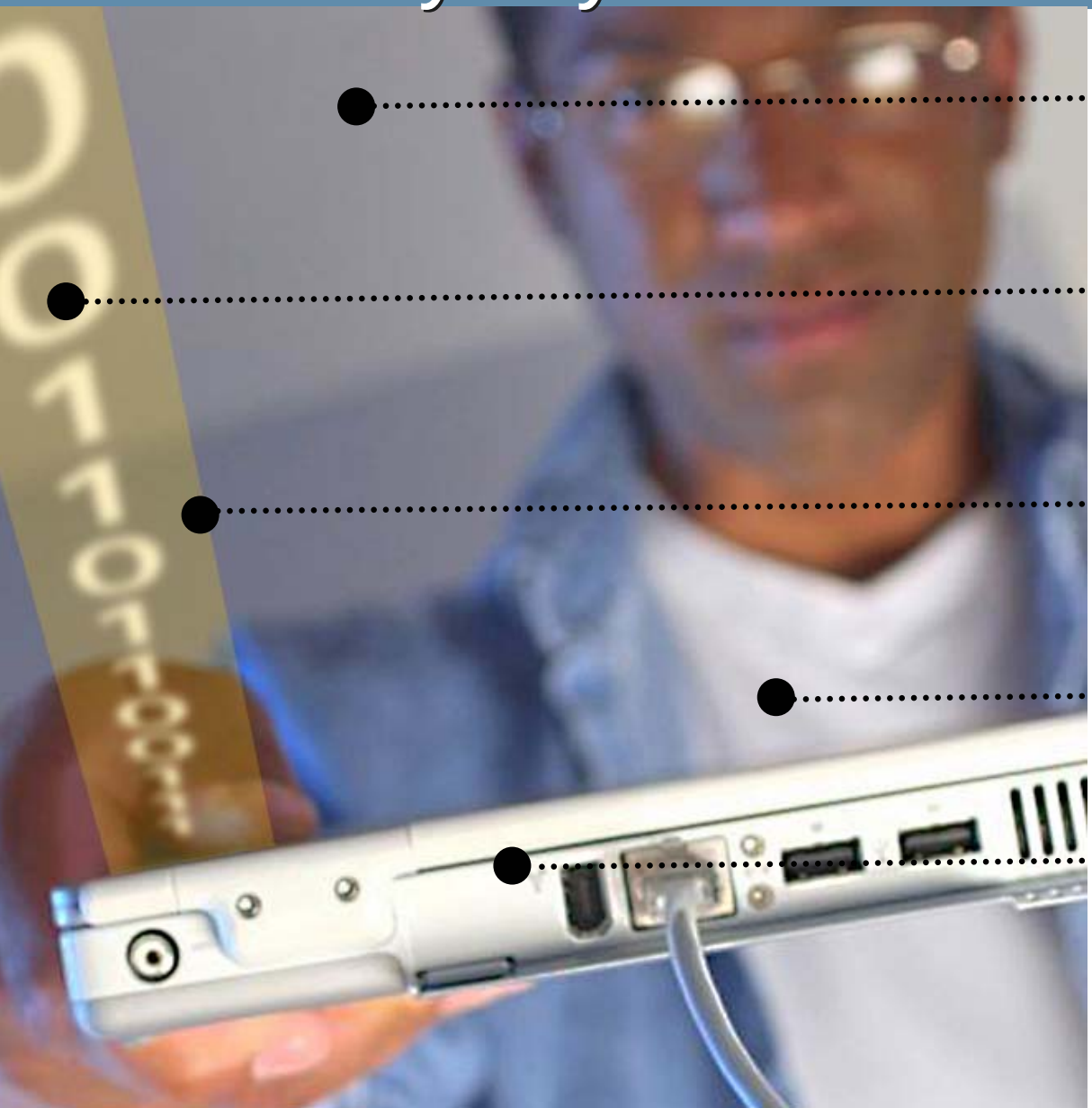


ARUBA WIRELESS NETWORKS

# Agenda

- Brief History
- WiFi Today
- WiFi Switching
- WiFi Switching Benefits
- RF Management
- Mobility
- Security
- Resources

# The Many Layers of Wireless Security



**Protecting the Air**
RF spectrum security, wireless IDS

**Protecting the Data**
Link layer encryption

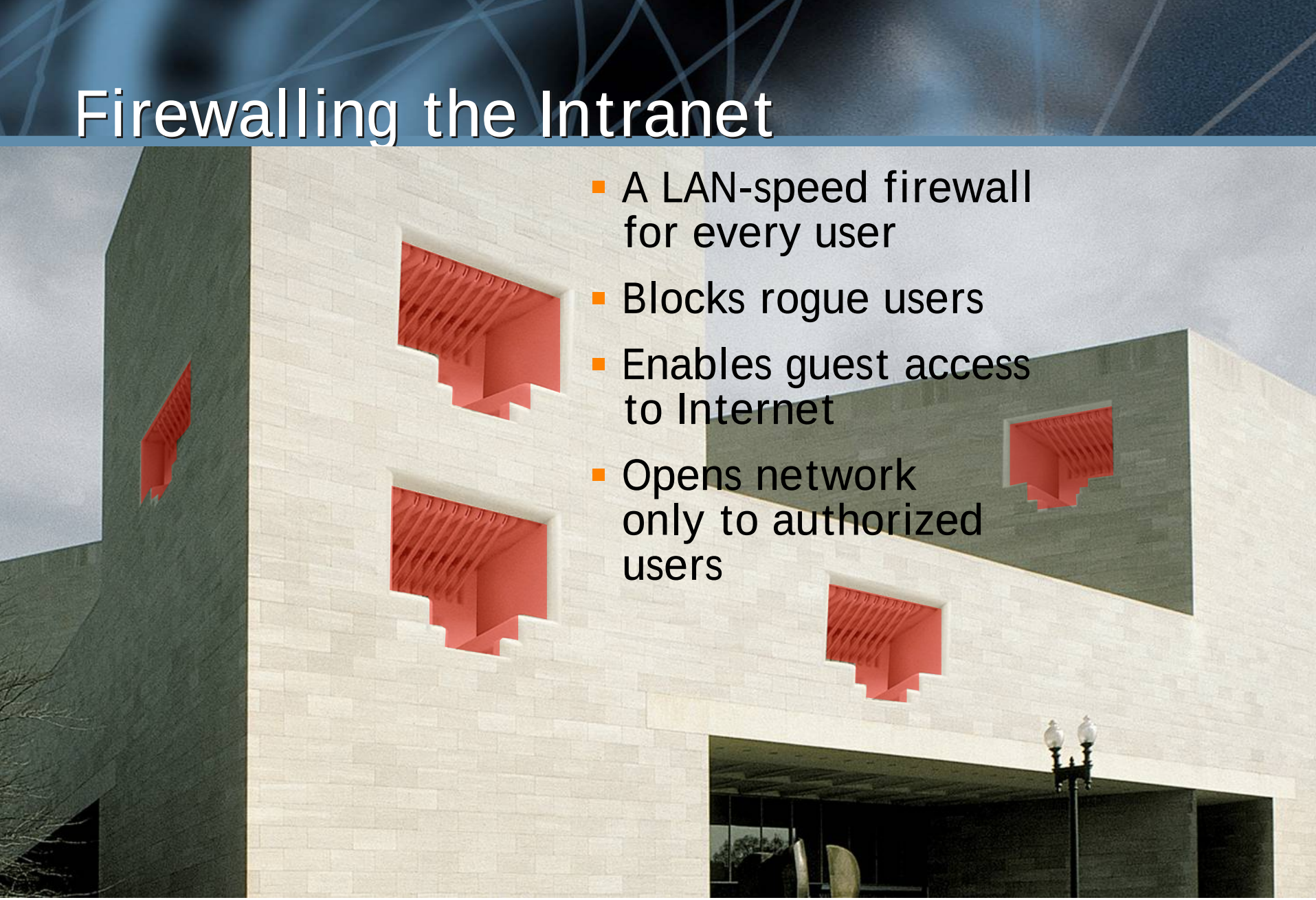
**Protecting the Connection**
Wireless VPNs

**Protecting the User**
Stateful per user firewalls

**Protecting the Network**
Client remediation
Device level authentication

ARUBA WIRELESS NETWORKS

# Firewalling the Intranet

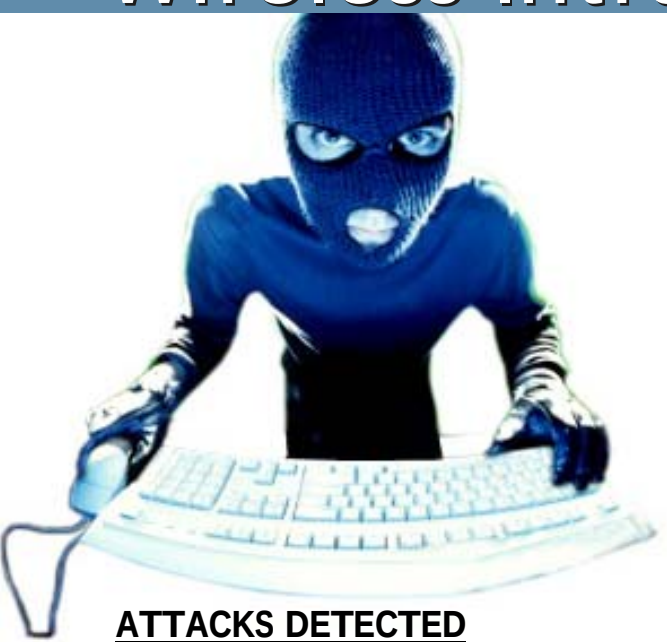


- A LAN-speed firewall for every user
- Blocks rogue users
- Enables guest access to Internet
- Opens network only to authorized users



ARUBA WIRELESS NETWORKS

# Wireless Intrusion Detection



**ATTACKS DETECTED**

- Netstumbler
- Fake AP flood
- Airjack
- Null SSID probe response
- Flood attacks
- Deauth broadcasts
- Station disconnect attacks
- Man-in-the-Middle attacks
- Wireless bridging
- Hotspotter
- Protection against adhoc networking

- Detection of anomalous frame rates
  - Excessive associate, disassociate, authenticate, deauthenticate, probe request/response frames
- Signature recognition of WLAN attack tools
- Detection of MAC address spoofing
- Detection of deviant WLAN topology

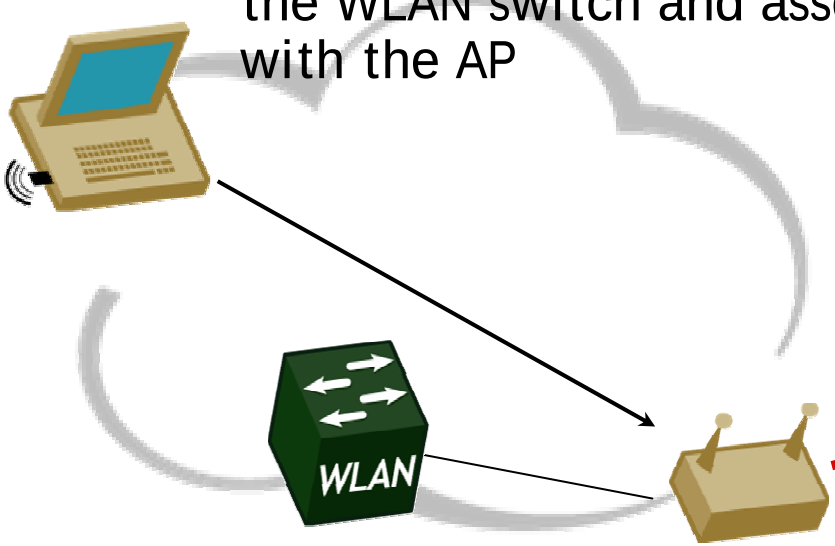


ARUBA WIRELESS NETWORKS

# Basic DoS Protection

## Protecting Against Flood Attacks

Legal client station is classified by the WLAN switch and associates with the AP




Unauthorized party floods deauthentication frames on behalf of client to the AP

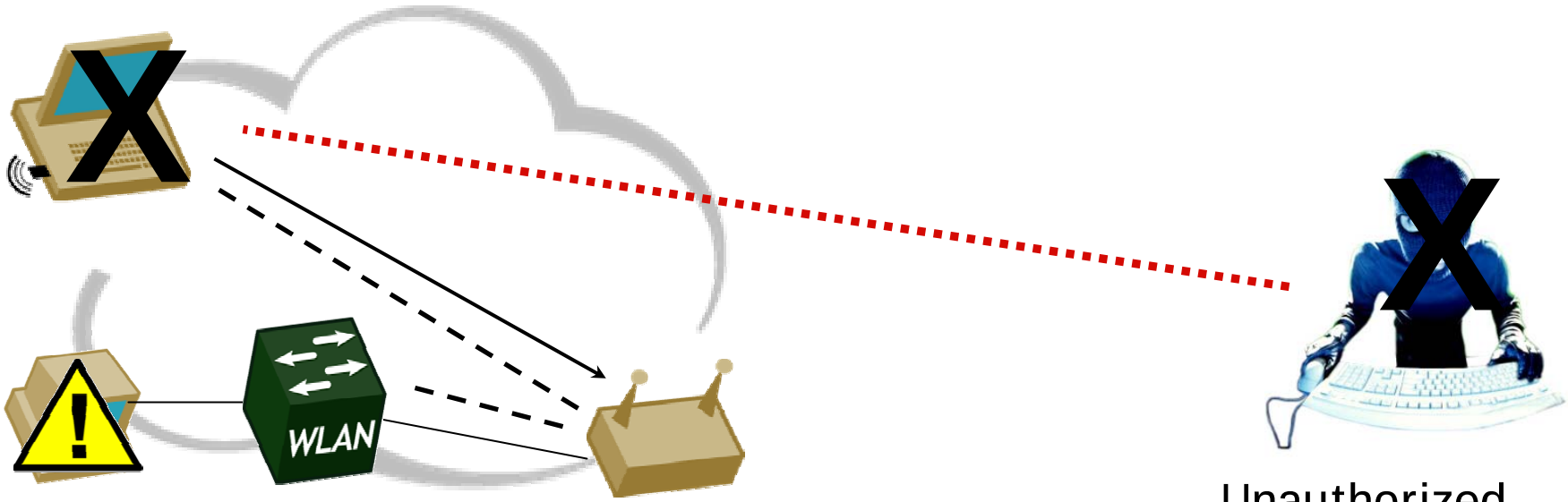
Based on location signature and client classification, the WLAN switch drops illegal deauthentication requests and generates alert



ARUBA WIRELESS NETWORKS

# Advanced DoS Protection

## Protecting Against the Man-in-the-Middle




Unauthorized party floods deauthentication frames on behalf of AP to client

The Wi-Fi switching system identifies illegal deauthentication frames sent to clients from unauthorized third-parties and blocks all future traffic sent from the station so hacker cannot obtain proprietary information like NT passwords. Wi-Fi switch generates alert to administrator.

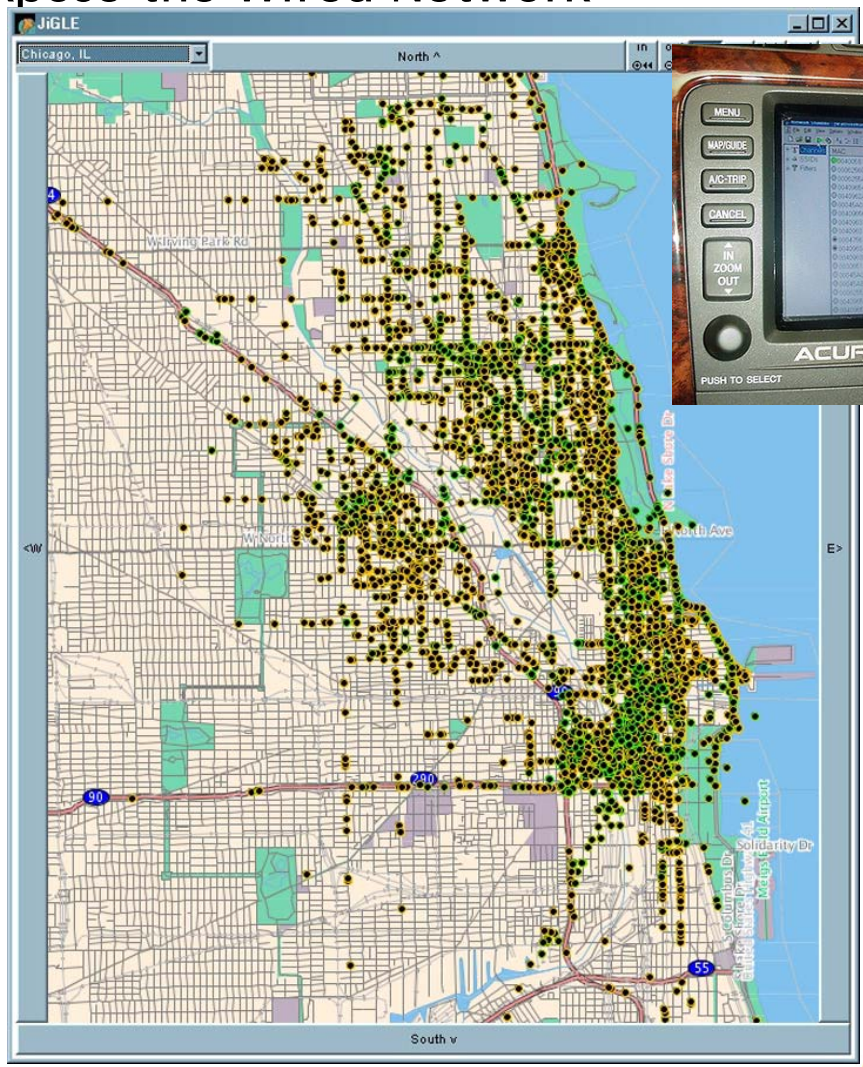


ARUBA WIRELESS NETWORKS

# War )( drove Lately ?

## Rogue Access Points expose the Wired Network

- Enterprise networks can be abused for SPAM
- ISP policies will shut down abusive enterprise networks
- Network resources can be exploited and DoSsed
- Sensitive data could be stolen

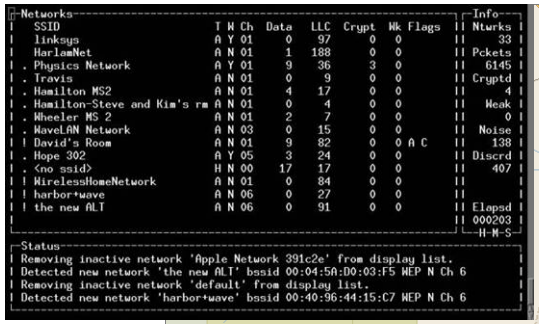




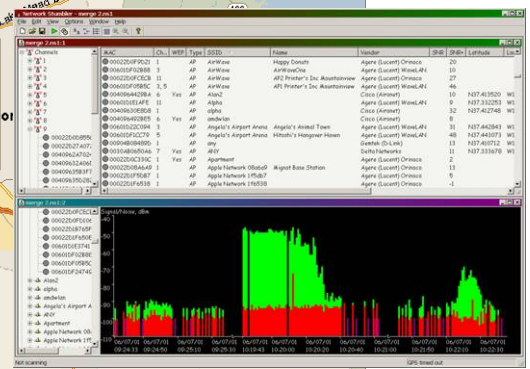


ARUBA WIRELESS NETWORKS

# Wardriving – Defcon 11 – Las Vegas, NV







Source: www.worldwidewardrive.org

# Second WWWD Numbers

| CATEGORY | TOTAL | PERCENT | PERCENT CHANGE |
|---|---|---|---|
| TOTAL APs FOUND | 24958 | 100 | N/A |
| WEP Enabled | 6970 | 27.92 | -2.21 |
| No WEP Enabled | 17988 | 72.07 | +2.21 |
| Default SSID | 8802 | 35.27 | +5.74 |
| Default SSID and No WEP | 7847 | 31.44 | +4.8 |
| Most Common SSID | 5310 | 21.28 | +2.31 |
| Second Most Common SSID | 2048 | 8.21 | +1.56 |

**Source: www.worldwidewardrive.org**

# Third WWWD Numbers

| Category | Total | Percent | Percent Change |
|---|---|---|---|
| Total AP Found | 88122 | 100 | +71.68 |
| WEP Enabled | 28427 | 32.26 | +4.34 |
| No WEP Enabled | 59695 | 67.74 | -4.34 |
| Default SSID | 24525 | 27.83 | -7.44 |
| Default SSID and No WEP | 21822 | 24.76 | -6.68 |

**Source: www.worldwidewardrive.org**



ARUBA WIRELESS NETWORKS

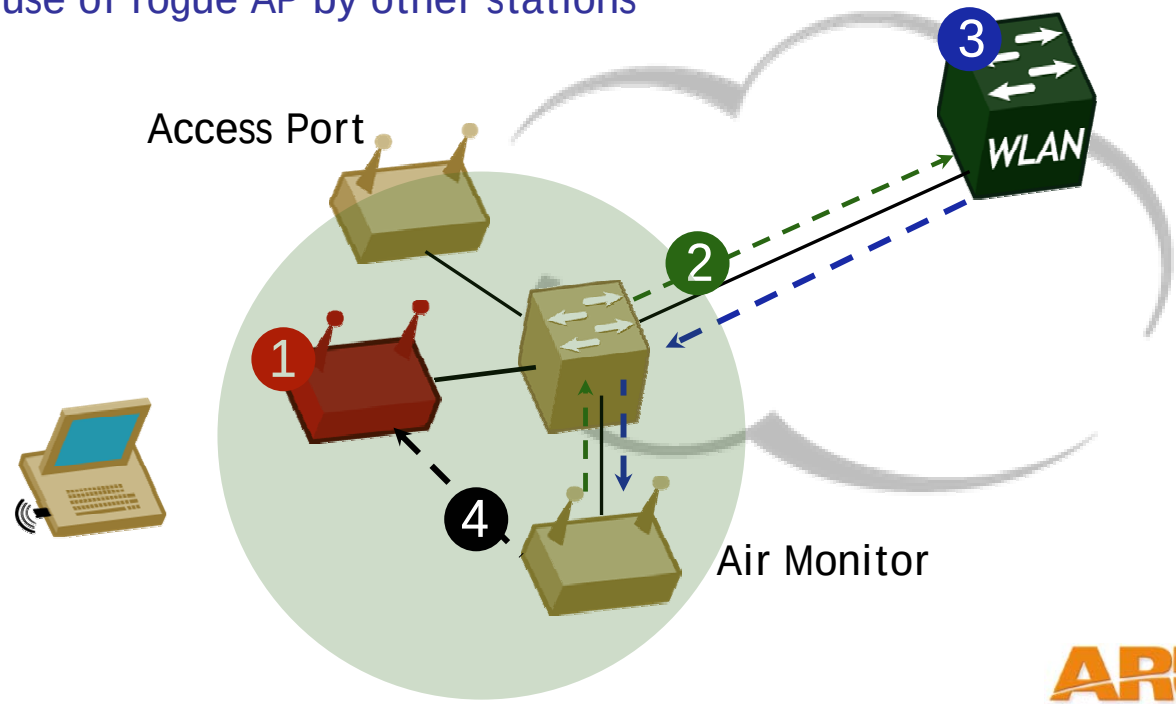
# Rogue AP Detection: Before



ARUBA WIRELESS NETWORKS

# Detecting and Preventing a Rogue AP

1. User plugs in unauthorized AP (rogue AP)
2. AM analyzes traffic in air to/from rogue AP and to/from wired network, classifies it as "rogue" or "interfering" and notifies WLAN switch
3. WLAN switch checks authorized user/device list and configuration policy and notifies AM to prevent user access through the rogue AP
4. AM sends disconnect packets to the client on behalf of the rogue AP and prevents future use of rogue AP by other stations

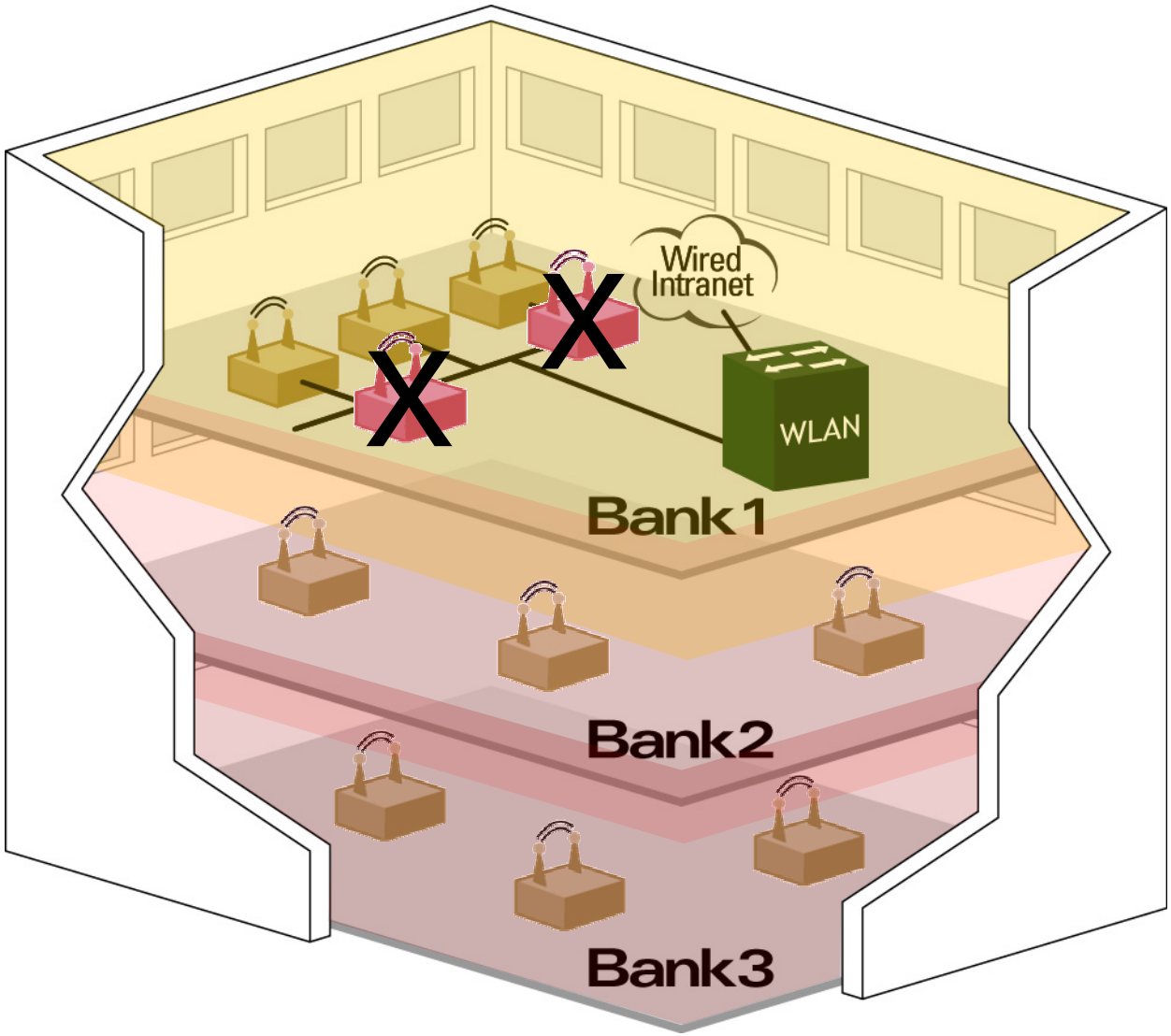





ARUBA WIRELESS NETWORKS

# Locking the Air

## Block Rogue Access Points and Hackers To Protect Your Air Space




Automatic
Wireless
Intrusion
Prevention



ARUBA
WIRELESS SYSTEMS

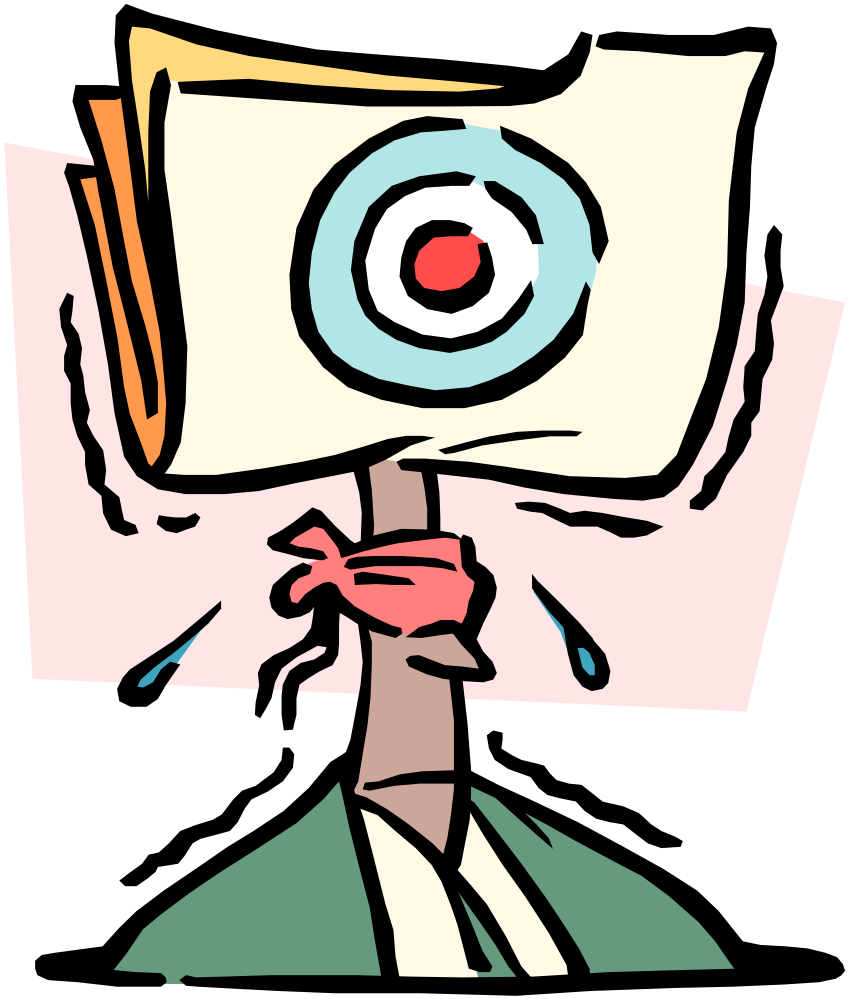
# Agenda

- Brief History
- WiFi Today
- WiFi Switching
- Using WiFi Switching
- Dynamic Coverage Detection and Calibration
- Mobility
- Security
- Resources

# Resources

- http://www.wi-fi.org
- http://www.unstrung.com/
- http://www.worldwidewardrive.org
- http://www.kismetwireless.net/
- http://www.netstumbler.com/
- http://www.wigle.net/
- http://nocat.net
- http://grouper.ieee.org/groups/802/11/

# Feedback?





ARUBA WIRELESS NETWORKS