

There's No Such Thing as A Trusted Network

Wireless Security in
the Enterprise

Randy Chou
Chief Security Architect



ARUBA
WIRELESS NETWORKS

Aruba At a Glance

- **Founded** February, 2002
- **Status** Privately-held, generating revenue
- **Funding** \$32 million (2 rounds)
- **Investors** Matrix Partners, Sequoia Capital
Trinity Ventures
- **Markets** WLAN infrastructure
- **Market Position** Centralized wireless security
- **Targets** Large Enterprise
and Wireless SPs
- **Innovation** First modular Wi-Fi
switching system
- **Employees** 100, Worldwide presence

Mobility: The Case For and Against



Improved
Productivity



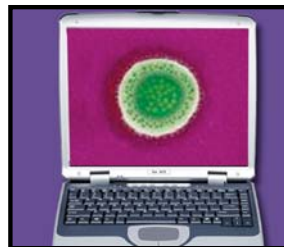
Ubiquitous
Voice and Data



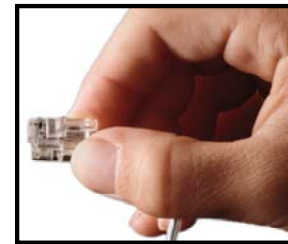
New
Mobile Apps



Unauthorized
Access

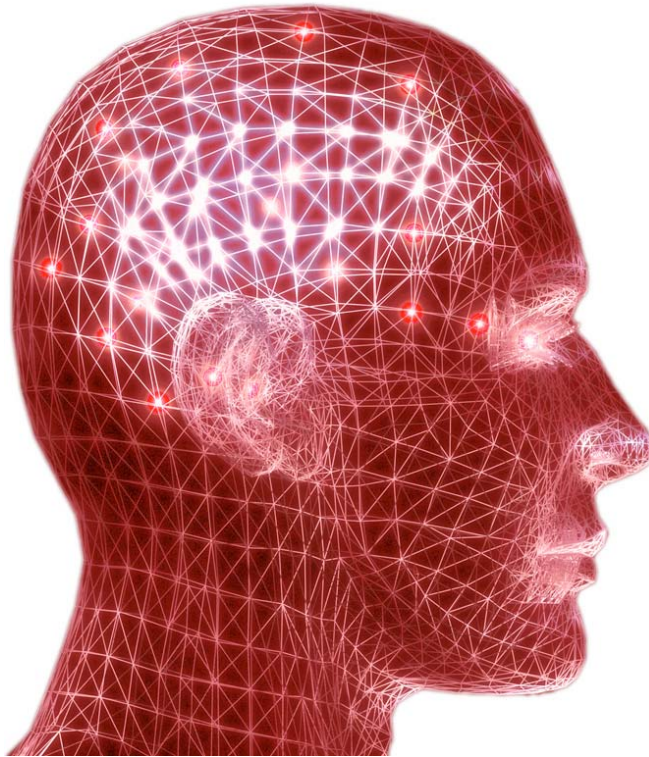


Worms and
Viruses



Rogue Access
Points

Mobility Changes Everything



- Requires rethinking security
- Requires rethinking network computing from a user perspective
 - Identity, location and presence are imperative
- Requires rethinking enterprise architecture for mobility

Mobility is All About the User

USER IDENTITY



Who the user is

USER LOCATION



Where the user is

USER PRESENCE

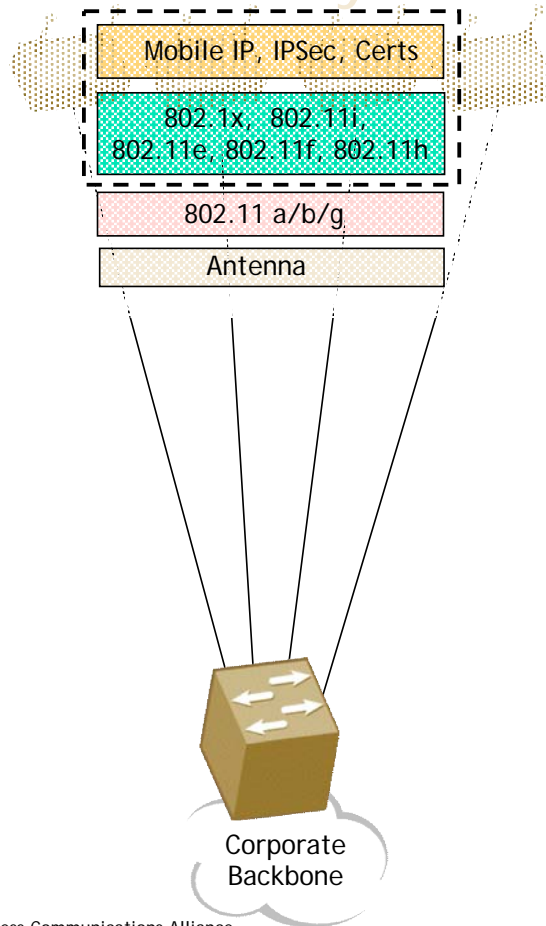


If the user is available

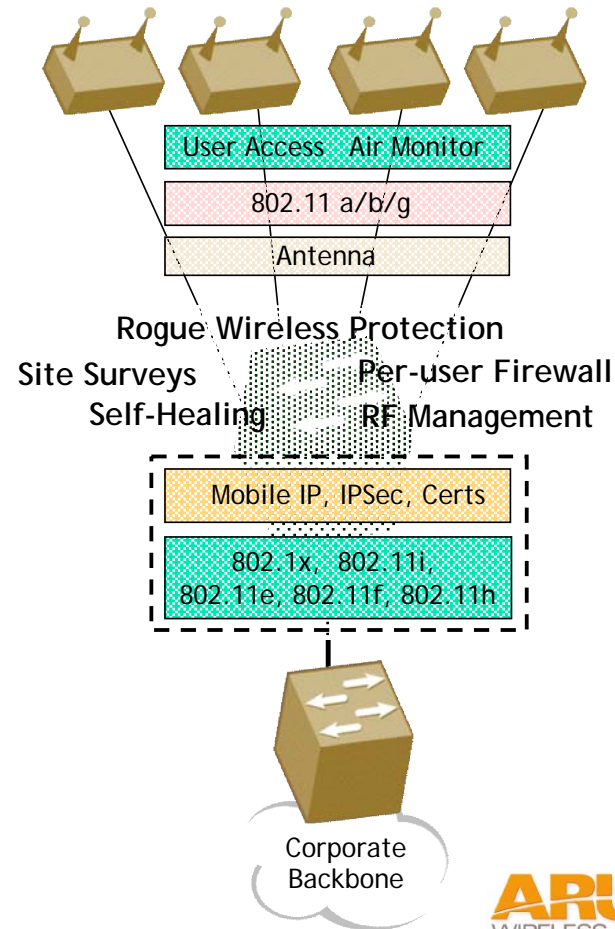


New Model for Enterprise Security

Today



Tomorrow



The Many Layers of Wireless Security

PROTECTING THE USER

Stateful Per User Firewalls

PROTECTING THE CONNECTION

IPSec, VPN

PROTECTING THE NETWORK

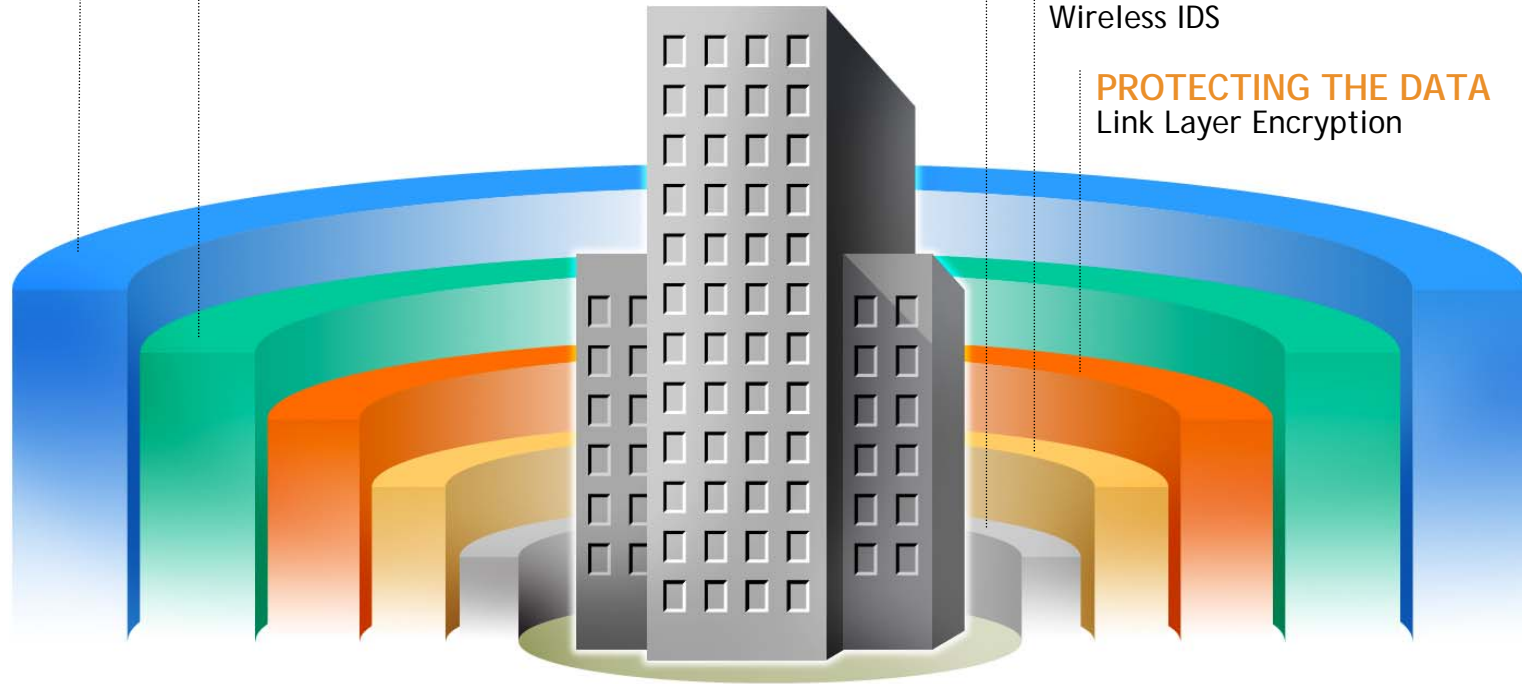
Device Level Authentication

PROTECTING THE AIR

RF Spectrum Security
Wireless IDS

PROTECTING THE DATA

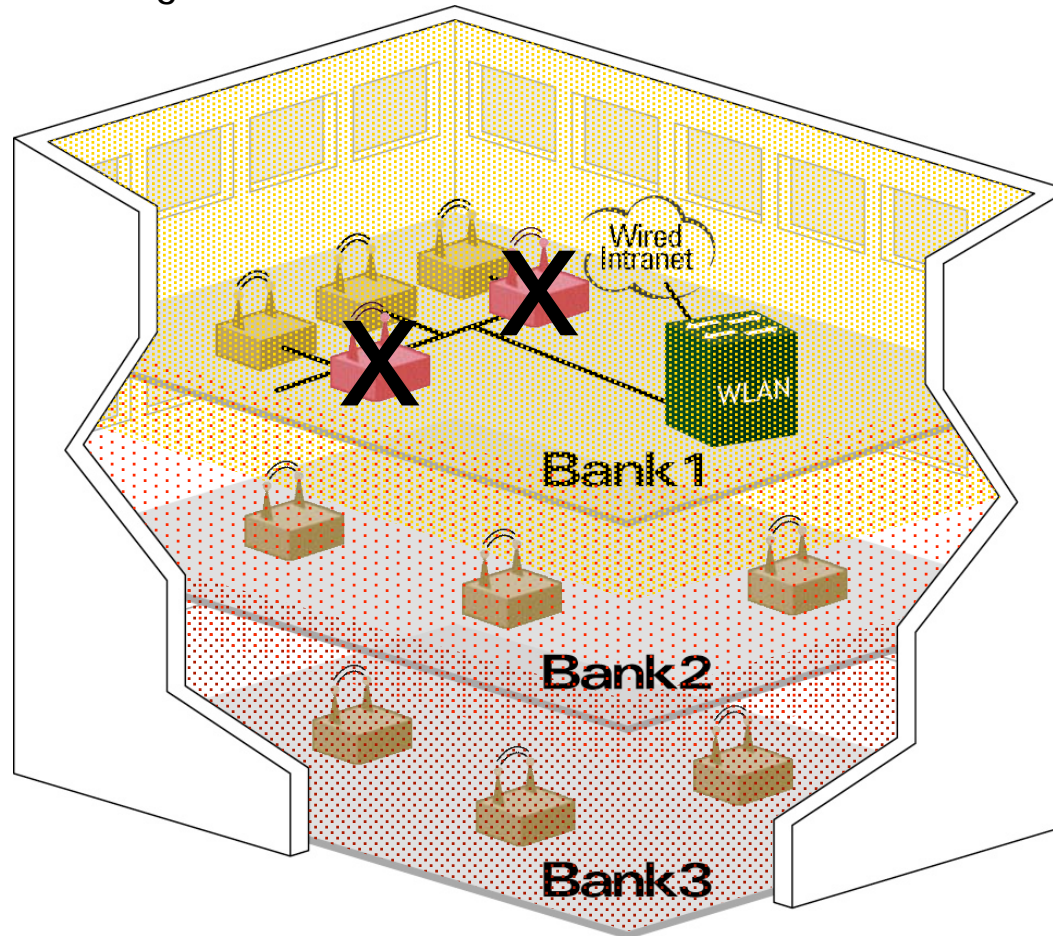
Link Layer Encryption



Enterprise Assets

Locking the Air

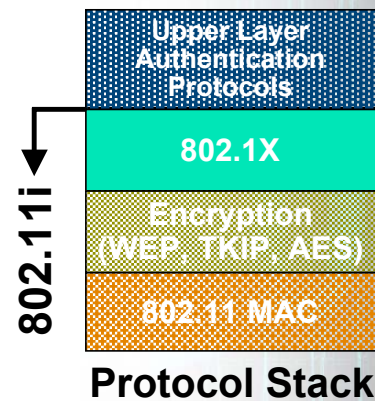
Block Rogue Access Points and Hackers To Protect Your Air Domain



Automatic
Wireless
Intrusion
Prevention

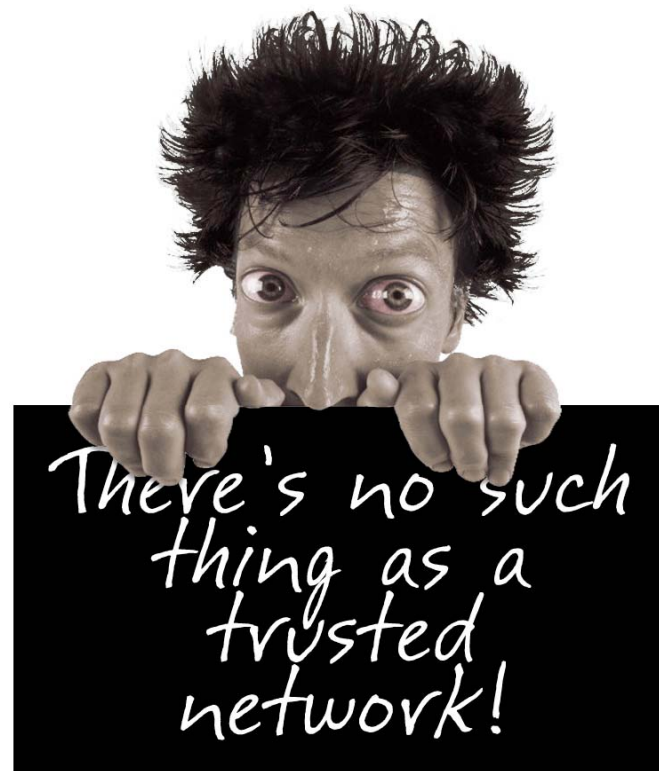
Protecting the Data

- **WPA / 802.11i**
 - ◆ Improved privacy (encryption algorithms)
 - ◆ Temporal Key Integrity Protocol (TKIP)
 - ◆ AES-CCMP-based encryption
 - ◆ Improved authentication and key distribution mechanisms
 - ◆ Using 802.1x



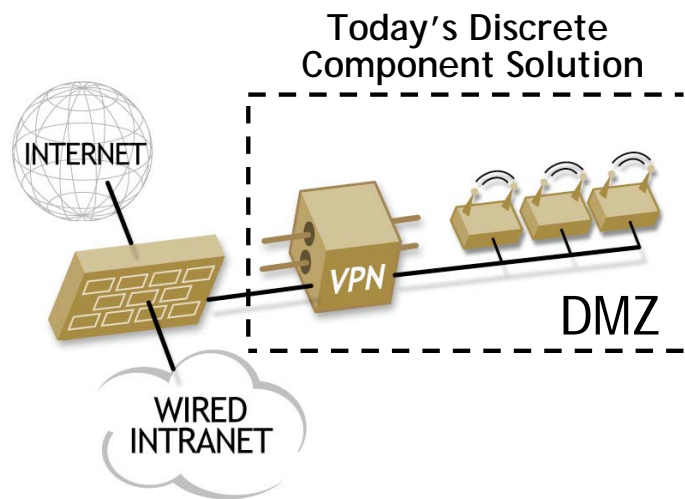
Protecting the User

- A LAN-speed firewall protects users from users
- Blocks rogue users
- Enables guest access to Internet
- Opens network only to authorized users

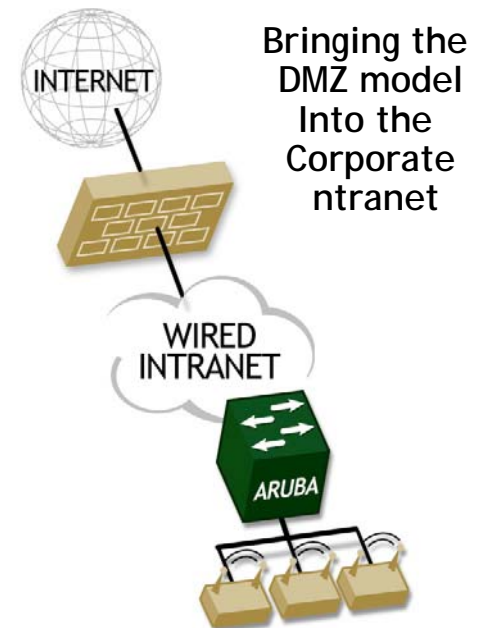


Protecting the Connection

Yesterday

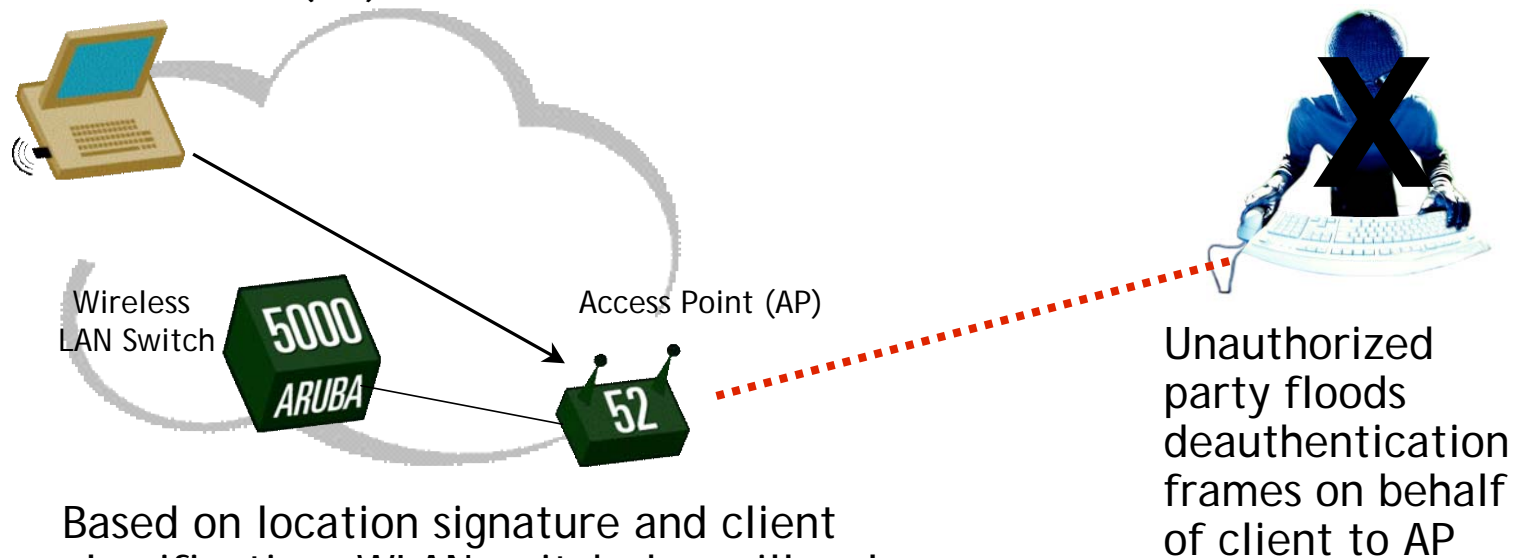


Today

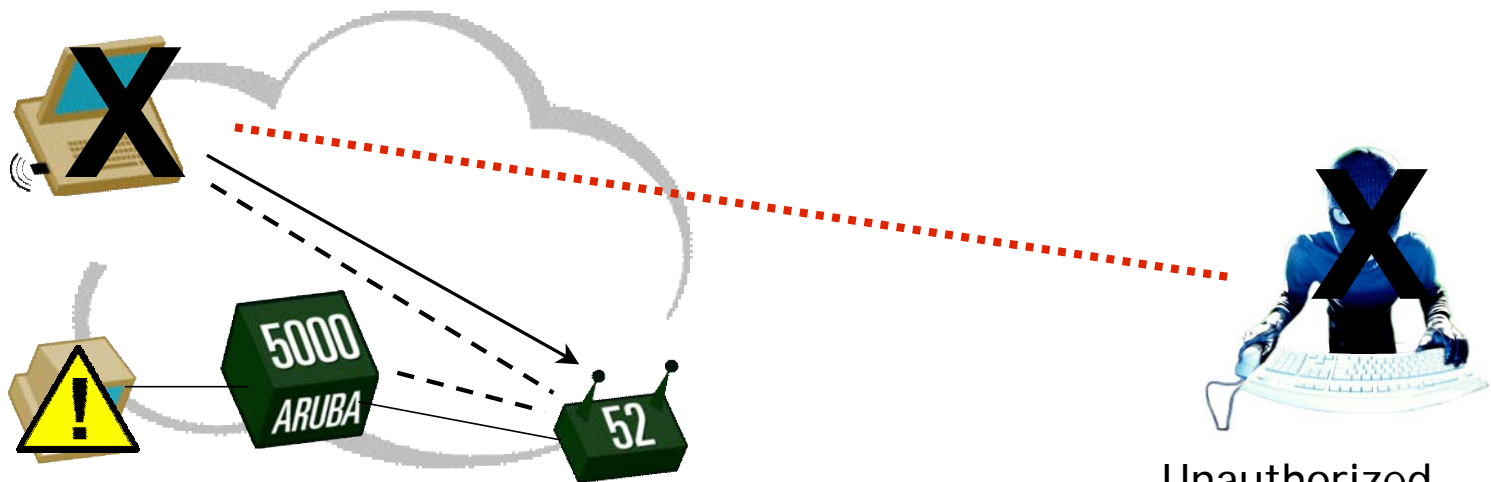


Protecting Against Floods

Legal client station is classified by a WLAN switch and associates with Access Point (AP)



Protecting Against Hackers

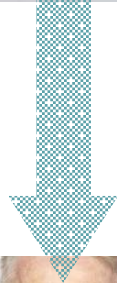
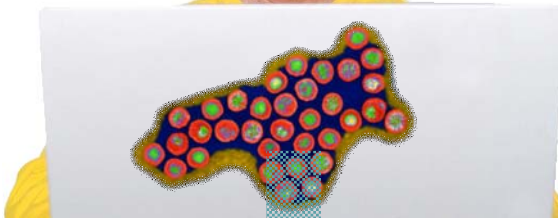


The Wi-Fi switching system identifies illegal deauthentication frames sent to clients from unauthorized third-parties and blocks all future traffic sent from the station so hacker cannot obtain proprietary information like NT passwords. Wi-Fi switch generates alert to administrator.

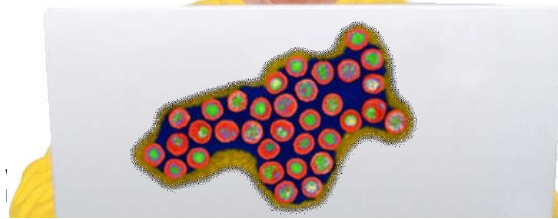
Unauthorized party floods deauthentication frames on behalf of AP to client

Wireless Virus Protection

UPS
employee



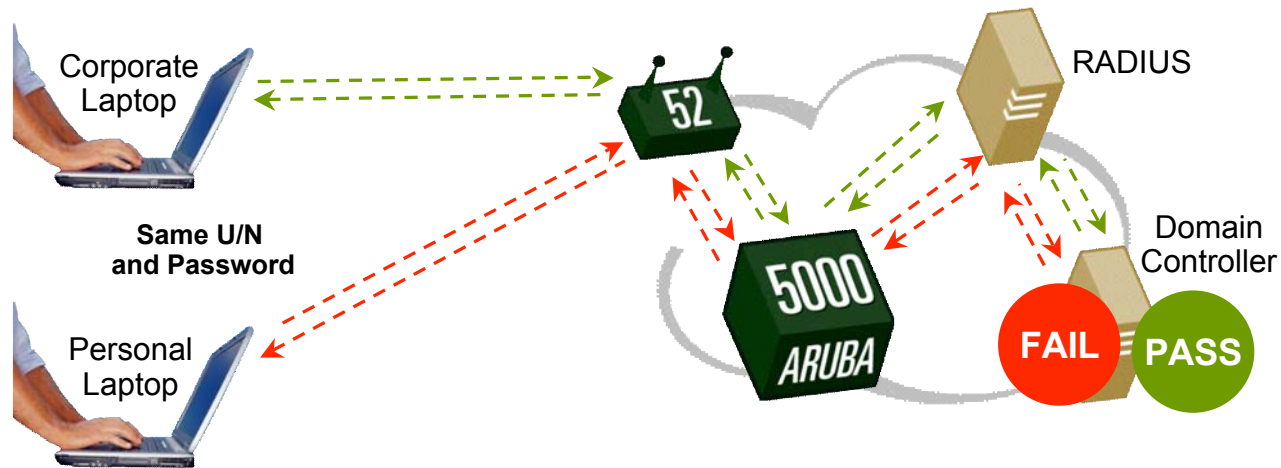
Same UPS
employee



- Ensuring endpoint integrity through automatic security checks
- Protecting the network from viruses by requiring stations to pass pre-defined security policies before entering the network
 - Pass = network access
 - Fail = redirection to URL for remediation
- Reduces enterprise exposure to security vulnerabilities and targeted attacks

Device Authentication

Ensures Only Authorized Devices Can Be Used to Access Network



- Adds another layer of security to wired/wireless networks
- Aruba enforces machine authentication before user authentication
- If the device cannot be authenticated, Aruba denies user(s) access or places in restricted role even if valid username and password has been provided
- Ideal for protecting against personal computers that are likely to be infected with viruses

Summary

- There's no holiday day for wireless security
- Multi-layered wireless security is needed
 - Physical RF security
 - Link layer encryption
 - VPN tunneling
 - User and device authentication
 - Mobile firewalling
- You can't secure what you can't see
- Rethink security based on user identity
- Centralization is a good thing