Roadmap to Wireless Network Security

Steve Walker

Iatric Systems

Seminar Overview

- Wireless Basic Overview
- Wireless Pitfalls
- Wireless Security
- Access Point Management
- VLANs
- Device Wireless Survey
- Stories From The Road

Wireless Networking
Can you hear me now?

- Most common is 802.11b/g (2.4Ghz)
- Less common is 802.11a (5.8Ghz)
- 11/54 Megabits in theory
- EMI Sensitive (Very)
- Usually implemented with an "Access Point"
- Very insecure "out of the box"

Wireless Security Pitfalls

- No barrier to entry (no wall jack to find)
- Data is accessible to anyone within range and with a proper NIC.
- 802.11b/g fair range, relatively cheap, many devices at same frequency
  - (microwave ovens, cordless phones, security radios/monitors)
- 802.11a shorter range, higher cost, fewer devices at same frequency

Solutions to Pitfalls
Creating barriers

- Authentication
  - WEP
  - MAC Address
  - Web Authentication
  - 802.1x + RADIUS

WEP

- Wired Equivalent Privacy
- Generally looked at as “better than nothing”.
- 64 & 128 bit, however 24 bits are used by the Initialization Vector (40 & 104).
- Limited number of IV’s leads to repetition of IV’s, thus allowing attackers to compare and extrapolate the key.
- Can you remember 26 character Hex key? Leads to users printing it “temporarily”

MAC Filtering

- Media Access Control address
  - Mostly unique address assigned to each NIC.
  - Normally the very first thing found by an attacker.
  - Most operating systems/NIC drivers have the ability to “spoof” a MAC address built in.

Web Authentication

- Typically best for guest-access situations
- Unless another encryption method is being used there is no data protection.
- Typically the website uses SSL and the username/password is encrypted.

802.1x

- Able to be used on wired and wireless installations
- Uses EAP, Extensible Authentication Protocol.
- Also referred to as “Port Based Authentication”
- Each step is encrypted and secured to ensure beginning to end security.
- Offers not only secure authentication but also secure data transfer.

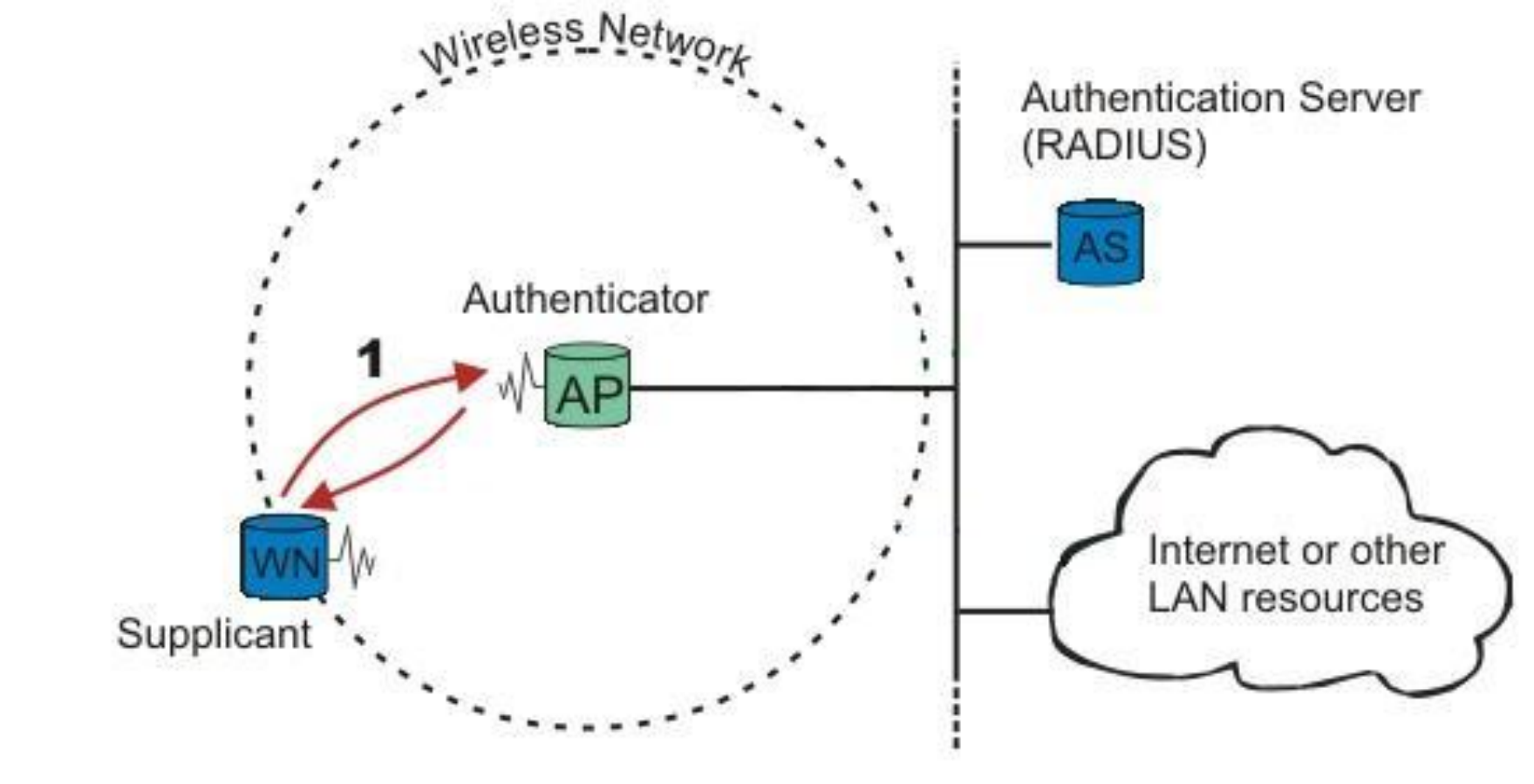
RADIUS

- Remote Authentication Dial-In User Service
- User information can be verified by querying a DC (ADS domain controller), LDAP, SQL, Kerberos, etc.
- Different options for a Radius server:
  - Microsoft Internet Authentication Service (IAS)
  - FreeRadius
  - Cisco Access Control Server (ACS)
  - OpenRadius

802.1x Step 1

- Authenticator sends an "EAP-Request/Identity“
- Supplicant sends an "EAP-Response/Identity“, that is automatically forwarded on to the Authentication Server (RADIUS)
- Authentication Server sends back a challenge to the Authenticator, who then unpacks this from IP and repackages it into EAPOL and sends it to the supplicant.

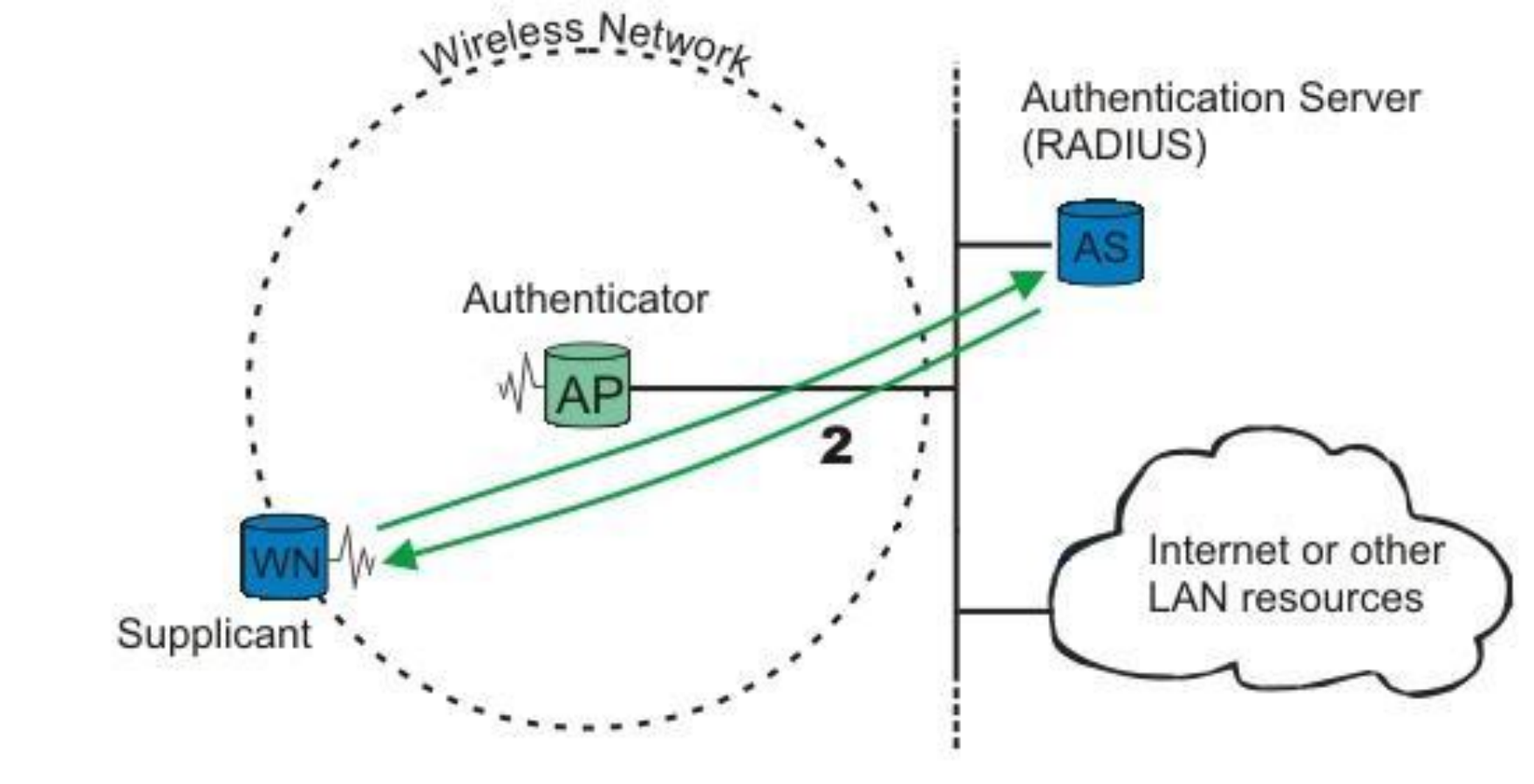
802.1x Authentication Process



802.1x Step 2

- Supplicant responds to the challenge via the Authenticator and passes the response onto the Authentication Server.
- If the Supplicant provides proper identity, the authentication server responds with a success message to the Supplicant.
- If the Supplicant does not provide proper identity the Authentication Server responds with a reject message and the Supplicant is not allowed access.

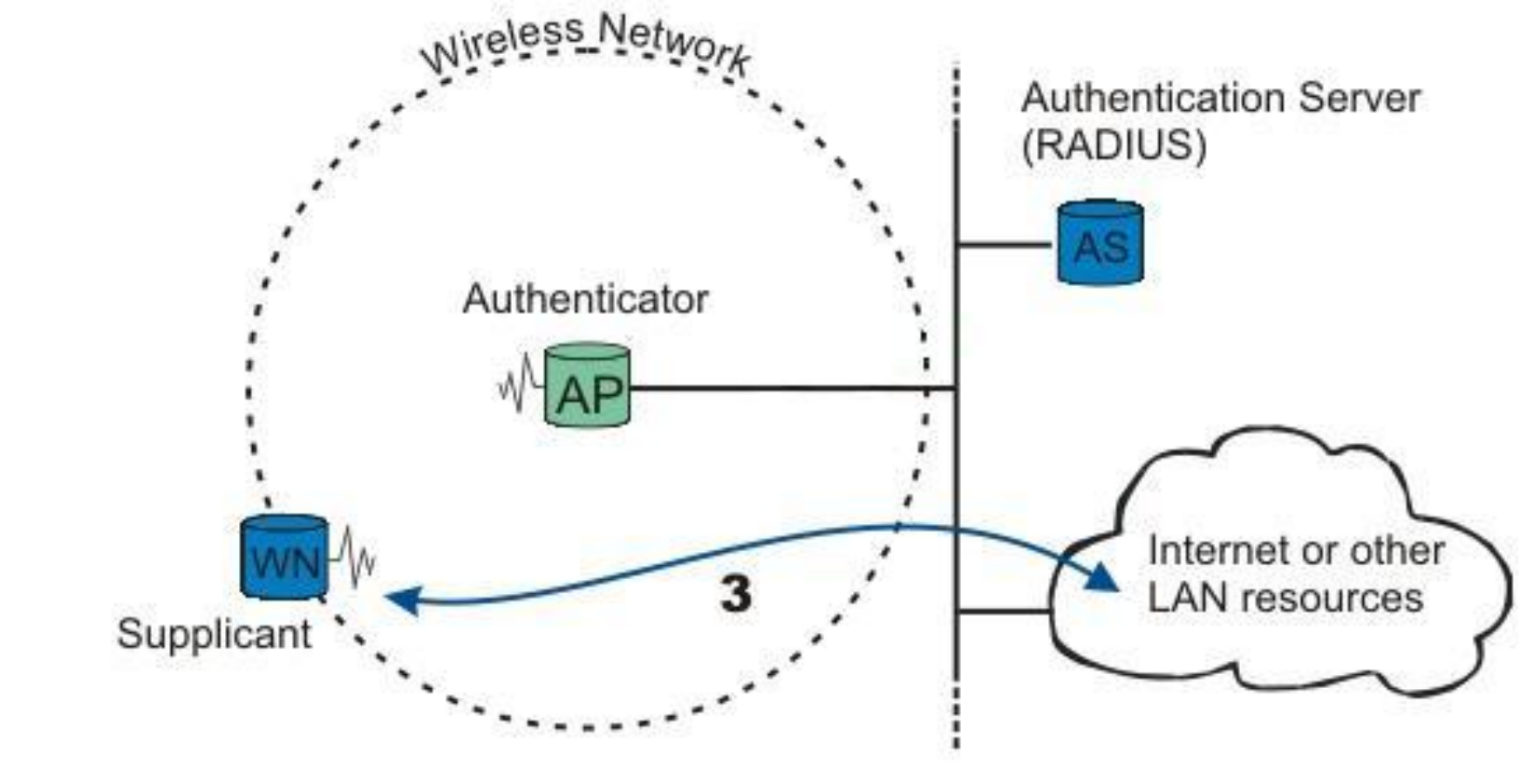
802.1x Authentication Process



802.1x Step 3

- Authenticator now allows the Supplicant access to the internet or other resources
- At this point the Authentication Server sends a Master Key and series of handshakes work to build the shared keys between the Supplicant and the Authenticator.

802.1x Authentication Process



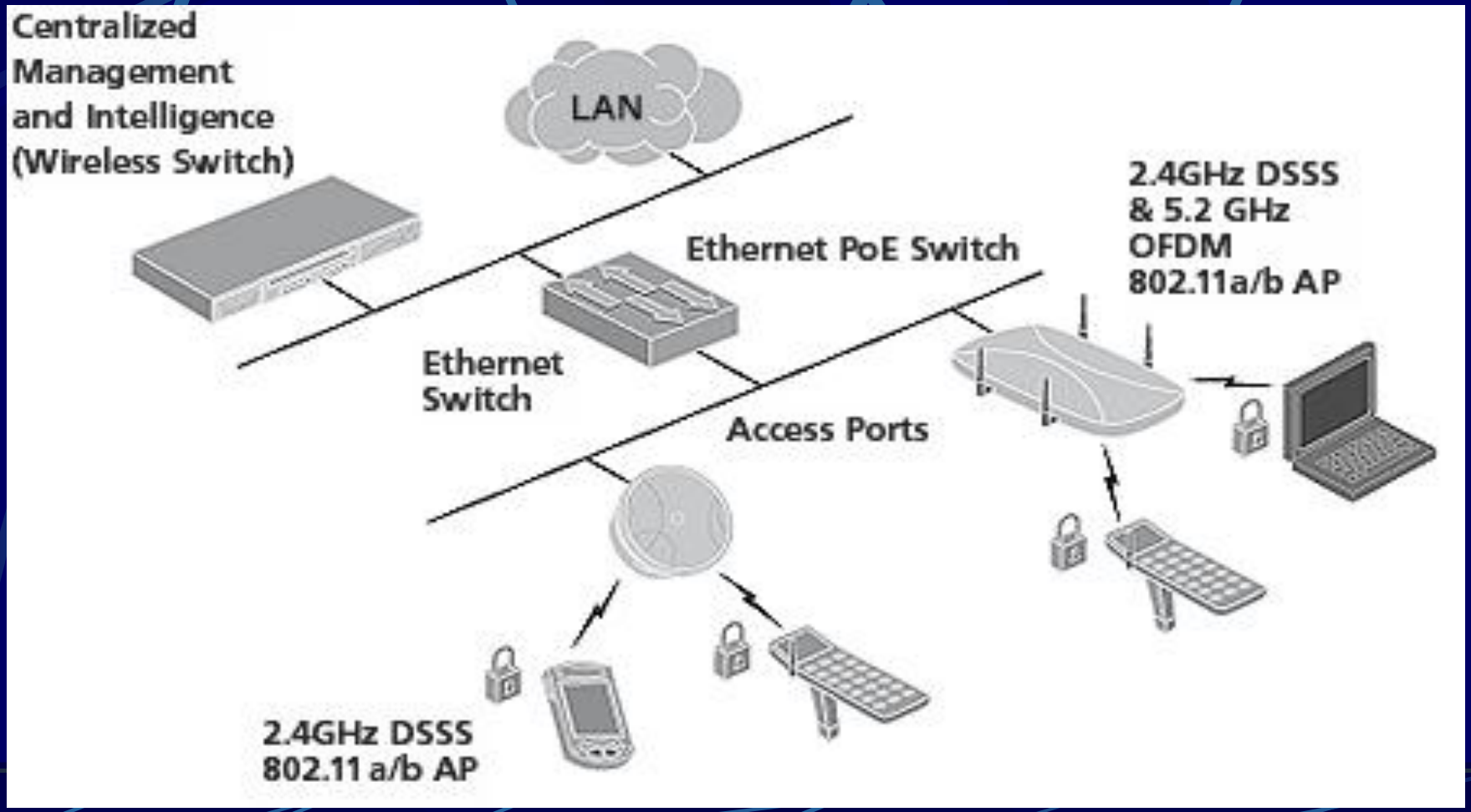
802.1x Support

- Windows XP – built in and only limited by NIC capabilities
- MAC OS X 10.3 began supporting natively.
- Most, if not all, Linux distributions have 802.1x support, only limited by NIC capabilities.

Wireless Access Point Management

- Thick Mode:
  - Fully Independent
  - Management is done at the AP level
  - Resembles most standard home APs
- Thin Mode
  - Light weight AP, limited number of low level functions (encryption, packet transmission, SSID announcement, etc.)
  - Centrally managed by a Wireless Switch Manager
  - Able to be placed anywhere on the network as long as they have a patch back to the Wireless Switch Manager

Wireless Access Point Management



VLAN

- Operate at Layer 2 of the OSI model, but normally configured to involve Layer 3 (IPs or Subnets)
- Logically another network, physically a switch or group of switches managed to be within the same logical network.
- VLANs can be used to control buildings, floors, groups of computers/users/resources.

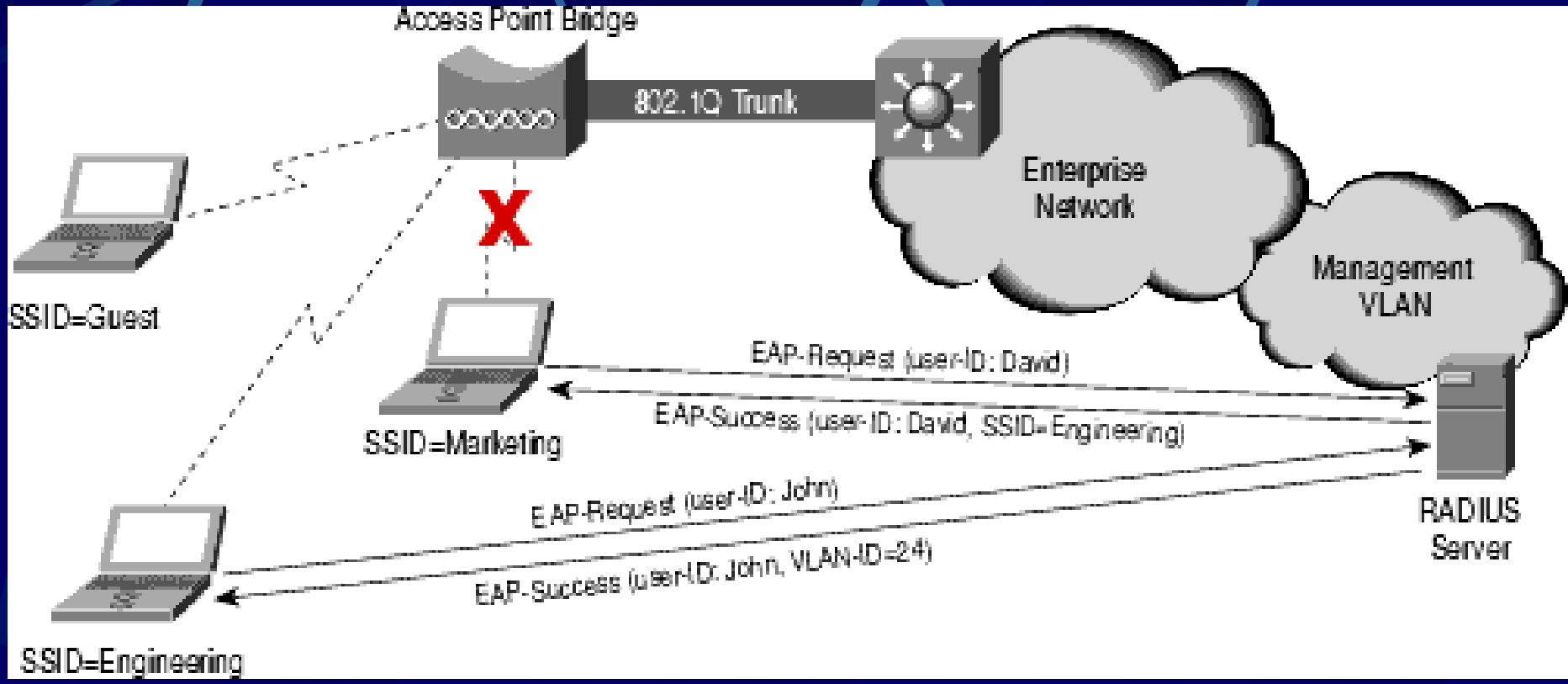
VLAN Wireless Application

- A VLAN can be associated with a specific SSID.
  - Even further, specific SSID user access can be controlled by including a RADIUS server.
- Instead of using multiple AP's for each SSID, 1 AP can handle multiple SSID/Networks.
- Each SSID can have different authentication/encryption standards applied. From open/guest access to 802.1x + dynamic WEP + TKIP/MIC.

VLAN Wireless Application

- In the following example multiple machines are accessing different SSIDs at the same AP
- David is attempting to connect to Marketing, however, RADIUS only shows him having access to Engineering. His connection is denied.
- John is attempting to connect to Engineering. RADIUS shows John has access to Engineering and is granted access.

VLAN Wireless Application



Device Wireless Capability Survey

	EAP Type				Encryption			Client Type(s)
Device	**TLS**	**TTLS**	**PEAP**	**LEAP**	**WEP**	**WPA**	**WPA2**	
Intermec CN2B	X	X	X	X	X	X	X	Intermec
Laptops	X		X		X	X	X	Windows
Laptops	X	X	X	X	X	X	X	Aegis
Palm Tungsten C				X	X			Aegis
Symbol PPT8846	X	X	X	X	X	X	X	Aegis
Symbol MC70	X	X	X	X	X	X	X	Aegis
Zebra QL220 Symbol 802.11b Radio				X	X	X		Zebra
Zebra QL220Plus Zebra or Symbol 802.11b Radio	X	X	X	X	X	X		Zebra
Zebra QL220Plus Zebra 802.11g Radio	X	X	X	X	X	X	X	Zebra

Stories

from the

Road