Optimizing Converged Cisco Networks (ONT)

WLAN Security, Management, & QoS

http://www.INE.com

WLAN Security Problems

- WLAN suffers from more security issues than traditional wired networks since…
  - Physical security is nearly impossible to implement
    - Anyone in range can potentially access the network, e.g. war driving
  - WLAN is a shared media
    - Sniffing tools are easy to implement, e.g. Aircrack-ng
- To overcome this, WLAN security must have two major goals
  - Stop unauthorized users from accessing the network
  - Authorized users' traffic shouldn't be compromised

WLAN Security Methods

- WLAN security features are similar to how IPsec VPNs work
  - Authentication
    - Only allow authorized users
  - Integrity checks
    - Prevent packets from being changed in the transit path
  - Confidentiality
    - Prevent others from reading the contents of packets
  - Anti-replay
    - Prevent packets from being re-sent
- Different implementations offer different combinations of these features
  - e.g. WEP vs. WPA

Wired Equivalent Protocol (WEP)

- Original 802.11 attempt at security
  - Authentication
    - Open (none) or Shared
  - Integrity
    - CRC checksum
  - Encryption
    - RC4 based stream cipher
    - 40, 104, or 128 bit key plus 24-bit Initialization Vector (IV)
      - Effective lengths of 64, 128, and 152 bits respectively
- Deprecated in today's networks
  - Keys are static and have no management protocol
  - Shared authentication is actually less secure than no authentication
  - Certain attacks can break WEP in < 1min

Cisco LEAP

- Lightweight Extensible Authentication Protocol
- Cisco proprietary stopgap for WEP
- Better authentication than WEP
  - 802.1x (RADIUS) for central management instead of static keys
- Better encryption & integrity than WEP
  - Cisco Key Integrity Protocol (CKIP)
    - Dynamic WEP key rotation
  - Cisco Message Integrity Check (CMIC)
- Like WEP, deprecated
  - Non-standard, so lack of client support
  - Still vulnerable to certain attacks

Wi-Fi Protected Access (WPA)

- Wi-Fi Alliance stopgap for WEP
  - Not an 802.11 standard
- Better authentication than WEP
  - "Personal" mode – PSKs
  - "Enterprise" mode – 802.1x for key management
- Better encryption & integrity than WEP
  - Temporal Key Integrity Protocol (TKIP)
    - Like CKIP, but standards based
    - Still RC4 based
  - Message Integrity Check (MIC)
    - Like CMIC, but standards based

Wi-Fi Protected Access Ver 2 (WPA2)

- 802.11i standard
- Better authentication than WEP
  - "Personal" mode – PSKs
  - "Enterprise" mode – 802.1x for key management
- Better encryption than WEP & WPA
  - Uses Advanced Encryption Standard and Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (AES-CCMP)
  - More hardware intensive, not all older client adapters and APs support it

802.1x Authentication

- Originally just for wired authentication
- Main advantage is centralized management and flexible methods
  - RADIUS for centralization
  - Extensible Authentication Protocol (EAP) for flexibility

EAP Variations

- EAP is a generic term, the actual implementations are…
  - Cisco LEAP
  - EAP-FAST
    - Flexible Authentication via Secure Tunneling
  - EAP-TLS
    - Transport Layer Security
  - PEAP-GTC
    - Protected EAP with Generic Token Cards
  - PEAP-MSCHAPv2
    - Protected EAP with Microsoft Challenge Handshake Authentication Protocol version 2

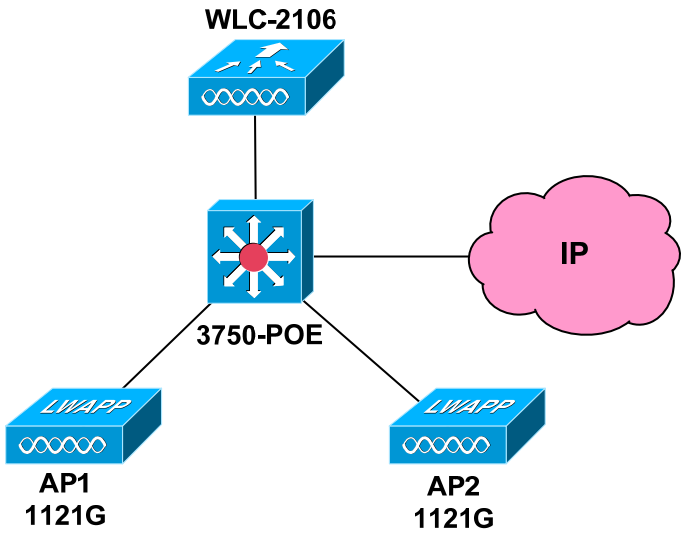
EAP Variations (cont.)

- Difference between variants is…
  - What database can you authenticate to
  - Are certificates required
  - Roaming support
- E.g. both EAP-FAST and EAP-TLS can use Active Directory, but TLS requires certificates

WLAN Management

- Typical problem with WLAN is centralized management
  - "Autonomous" APs must maintain their own configs
  - Some control through CiscoWorks Wireless LAN Solution Engine (WLSE)
- Main advantage of CUWS is that management is centralized
  - LWAPs are plug-and-play
  - WLC controls LWAPs configurations
  - Cisco Wireless Control System (WCS) manages multiple WLCs
    - Advanced applications like Location Service can tell you where a client is physically located in the network

WLAN Example



WLAN QoS

- Like in the wired network, proper end-to-end classification is needed to enforce a DiffServ policy
- Wired classification is no problem
  - Layer 2 CoS
  - Layer 3 IP Precedence & DSCP
  - Layer 4 & NBAR
- How do we extend this to the WLAN?
  - Answer: Wi-Fi Multimedia (WMM) and 802.11e

WMM & 802.11e

- Extends markings into 802.11 header
- WMM uses four access categories
  - Voice, video, background, & best effort
  - Subset of the 802.11e spec
- 802.11e uses eight priority levels
  - 6 & 7 map to WMM Voice
  - 4 & 5 map to WMM Video
  - 1 & 2 map to WMM Background
  - 0 & 3 map to WMM Best Effort

WLAN Queueing & DCF

- Per CSMA/CA logic, WLAN queueing is…
  - Wait for free RF, then transmit
  - Other stations must wait Frame Duration + DIFS + Random Backoff
- Logic queues can be created changing DIFS and Random Backoff timers
  - Lower IFS and lower Backoff means faster and more often transmission, hence higher priority

WMM & 802.11e EDCF

- WMM & 802.11e introduces Extended Distributed Coordinated Function (EDCF)
- EDCF replaces DIFS + Backoff with…
  - Short Inter-Frame Spacing (SIFS)
  - Fixed wait time
  - Random backoff timer
- After normal frame duration, transmitting host must wait SIFS + fixed wait + random backoff
- Logical queues are achieved by varying fixed wait time and random backoff per classification
  - E.g. “platinum” traffic has shorter fixed wait time and smaller random backoff range than “bronze” traffic

802.11e to L2 & L3 Mappings

- To achieve end-to-end classification, WLAN queue should correlate to L2 CoS & L3 DSCP
- For Lightweight WLANs, this is accomplished in…
  - Client towards WLC
    - LWAP copies 802.11e marking to outer DSCP field of LWAPP tunnel
    - WLC copies inner DSCP to Layer 2 CoS (802.1p)
  - WLC towards client
    - WLC copies 802.1p and DSCP to outer 802.1p and DSCP of LWAPP tunnel
    - LWAP copies outer DSCP of LWAPP tunnel to 802.11e

Key 802.11e Mappings

- By default, LWAP and WLC map…
  - DSCP EF to 802.1p 5 and 802.11e 6
  - DSCP AF31 to 802.1p 3 and 802.11e 4
  - DSCP 0 to 802.1p 0 and 802.11e 0 & 3
- This means that…
  - VoIP (EF) is in the highest queue
  - VoIP Control (AF31) is second highest
  - Scavenger (0) is in lowest queue
- On WLC QoS policy can also be applied overall to an entire SSID and to queue depths
  - E.g. SSID “VoIP” is always in “platinum”

WLAN Security, Management, & QoS Q&A