IEEE 802.1X For Wireless LANs

Bernard Aboba, Tim Moore, Microsoft
John Roese, Ravi Nalmati, Cabletron
Albert Young, 3Com
Carl Temme, Bill McFarland, T-Span
David Halasz, Aironet
Paul Congdon, HP
Andrew Smith, Extreme Networks

Outline

- Deployment issues with 802.11
- Adaptation of IEEE 802.1X to 802.11
- Summary

Deployment Issues With 802.11

- User administration
  - Integration with existing user administration tools required (RADIUS, LDAP-based directories)
    - Create a Windows group for wireless
    - Any user or machine who is a member of the group has wireless access
  - Identification via User-Name easier to administer than MAC address identification
  - Usage accounting and auditing desirable
- Key management
  - Static keys difficult to manage on clients, access points
  - Proprietary key management solutions require separate user databases

Security Issues With 802.11

- No per-packet authentication
- Vulnerability to disassociation attacks
- No user identification and authentication
- No central authentication, authorization, accounting
- RC4 stream cipher vulnerable to known plaintext attack
- Some implementations derive WEP keys from passwords
- No support for extended authentication
  - Token cards, certificates, smartcards, one-time passwords, biometrics, etc.
- Key management issues
  - Re-key of global keys
  - No dynamic per-STA key management

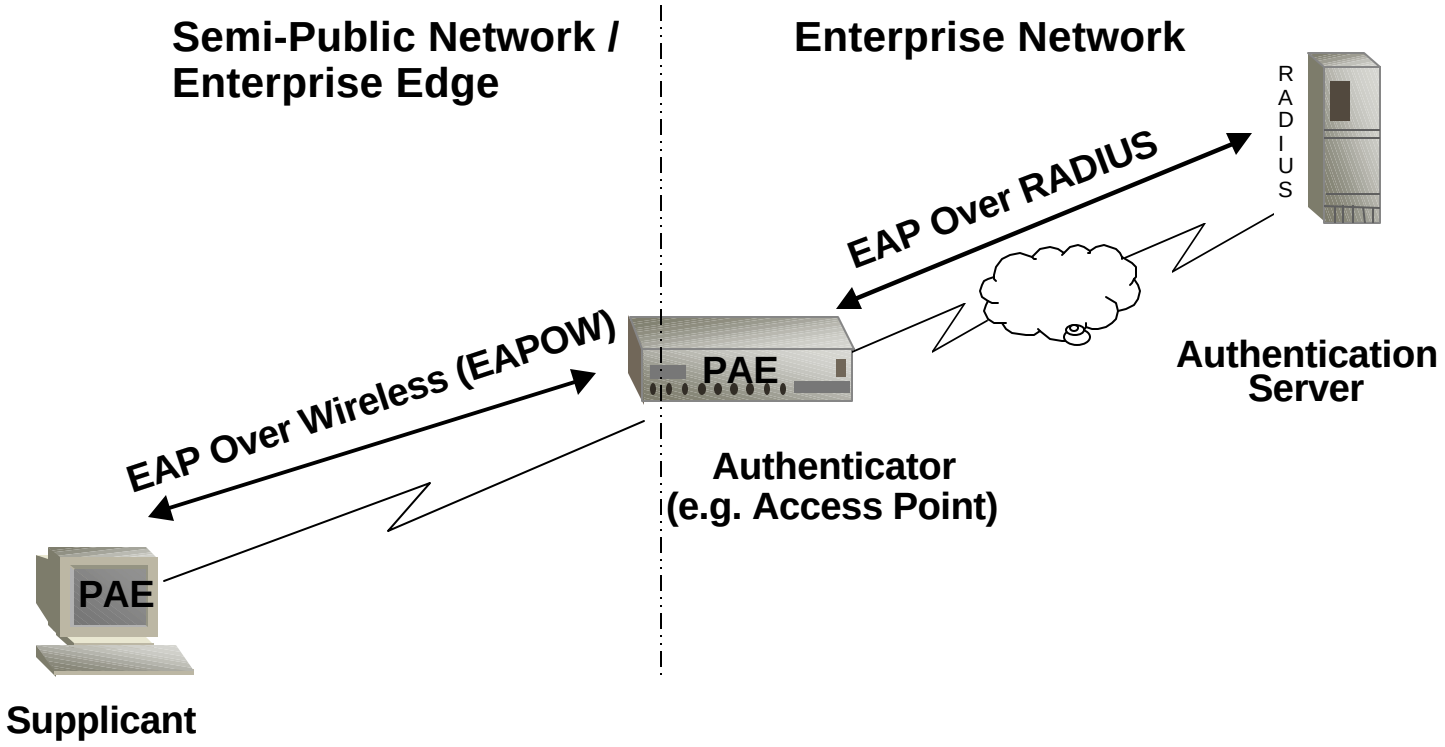
Advantages of IEEE 802.1X

- Open standards based
  - Leverages existing standards: EAP (RFC 2284), RADIUS (RFC 2138, 2139)
  - Enables interoperable user identification, centralized authentication, key management
- User-based identification
  - Identification based on Network Access Identifier (RFC 2486) enables support for roaming access in public spaces (RFC 2607).
- Dynamic key management
- Centralized user administration
  - Support for RADIUS (RFC 2138, 2139) enables centralized authentication, authorization and accounting
  - RADIUS/EAP (draft-ietf-radius-ext-07.txt) enables encapsulation of EAP packets within RADIUS.

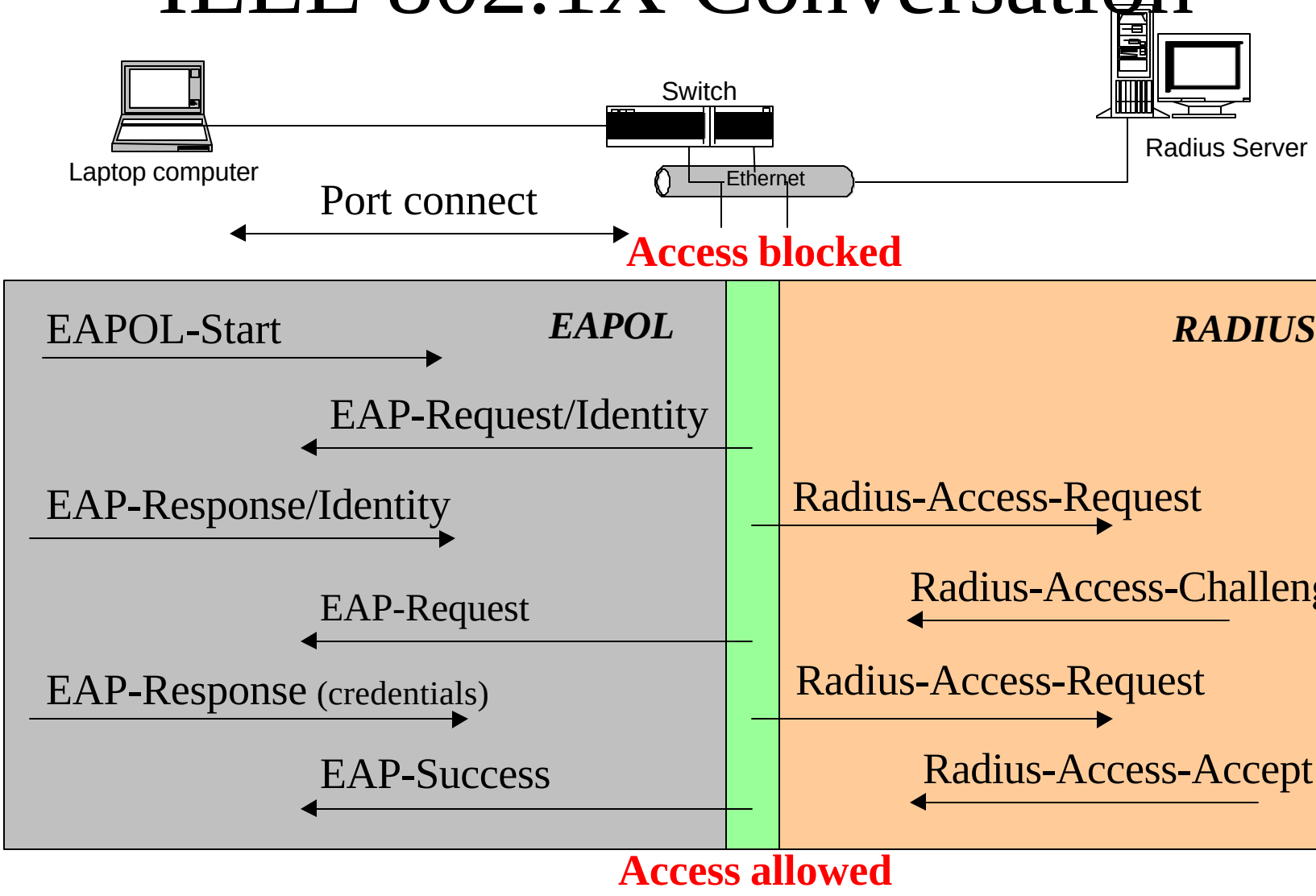
Advantages of IEEE 802.1X, cont'd

- Extensible authentication support
  - EAP designed to allow additional authentication methods to be deployed with no changes to the access point or client NIC
  - RFC 2284 includes support for password authentication (EAP-MD5), One-Time Passwords (OTP)
  - Windows 2000 supports smartcard authentication (RFC 2716) and Security Dynamics

802.11 General Topology



IEEE 802.1X Conversation



Goals for 802.1X on 802.11 Wireless LANs

- Minimal changes required to 802.1X and 802.11 specifications
  - 802.1X protocol same over 802.3 as 802.11
- Client access control
  - Support for both user and machine access control
- Centralized user administration
  - RADIUS client support on Access Point
- Management of encryption keys
  - Transmission of global/multicast keys from access point to client
  - Dynamic derivation of unicast keys
- Roaming support
- Ad-hoc networking support

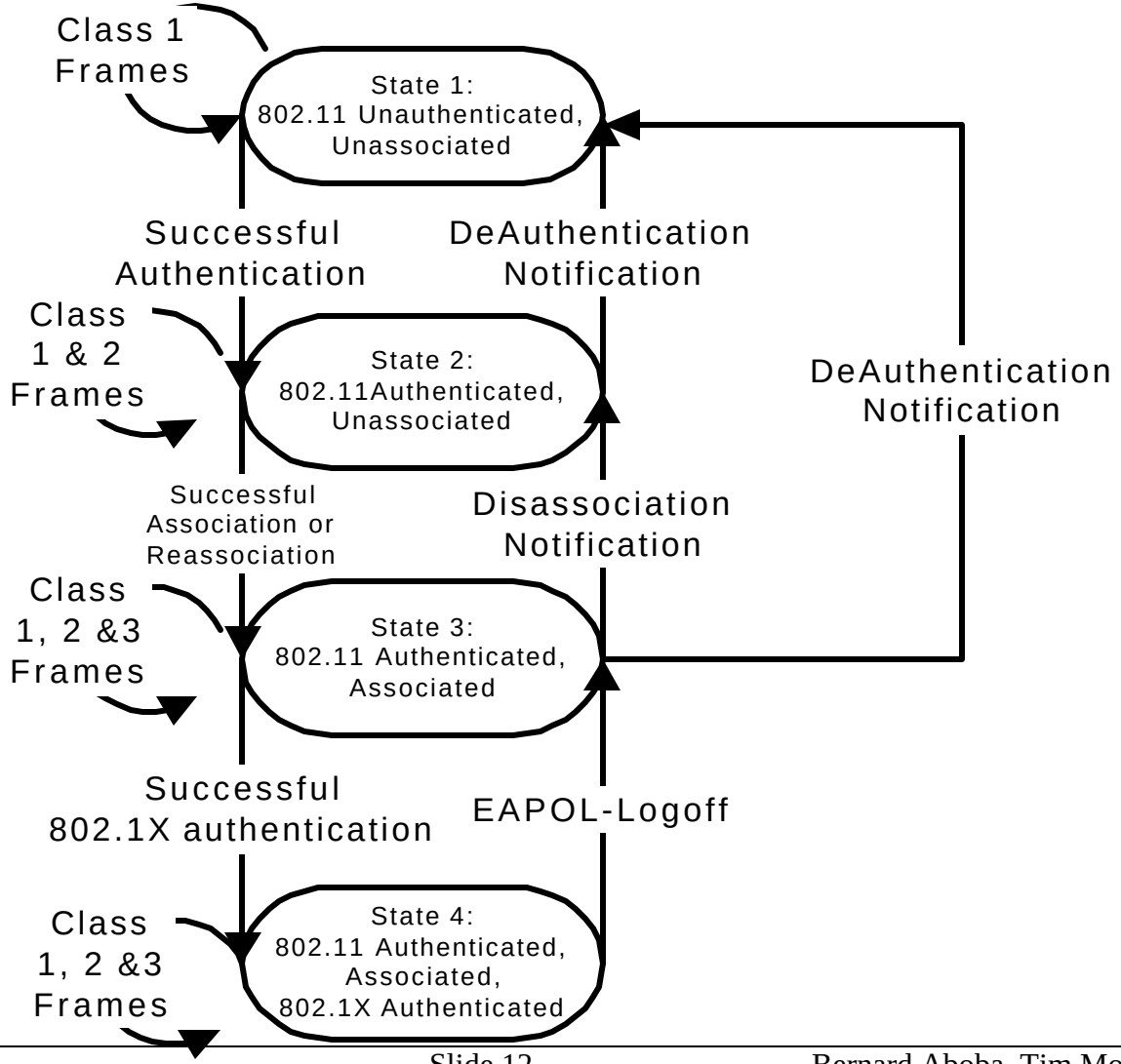
802.11 association

- Access point configured to allow open and shared authentication
- Initial client authentication
  - Open authentication used, since dynamically derived WEP key not yet available
- Client associates with access point

802.1X authentication in 802.11

- IEEE 802.1X authentication occurs after 802.11 association
  - After association, client and access point have an Ethernet connection
  - Prior to authentication, access point filters all non-EAPOL traffic from client
  - If 802.1X authentication succeeds, access point removes the filter
- 802.1X messages sent to destination MAC address
  - Client, Access Point MAC addresses known after 802.11 association
    - No need to use 802.1X multicast MAC address in EAP-Start, EAP-Request/Identity messages
  - Prior to 802.1X authentication, access point only accepts packets with source = Client and Ethertype = EAPOL

802.11/802.1X State Machine



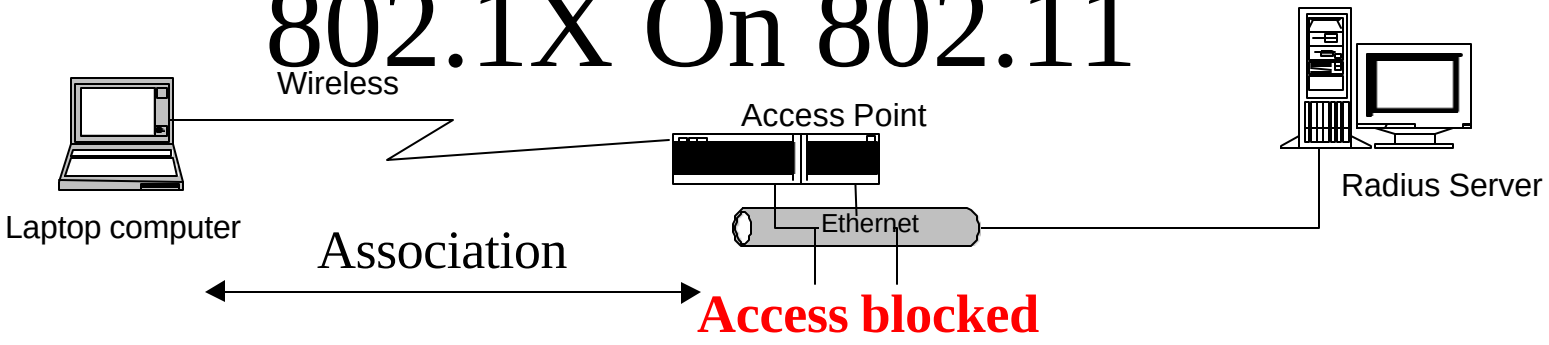
802.1X and Per-STA Session Keys

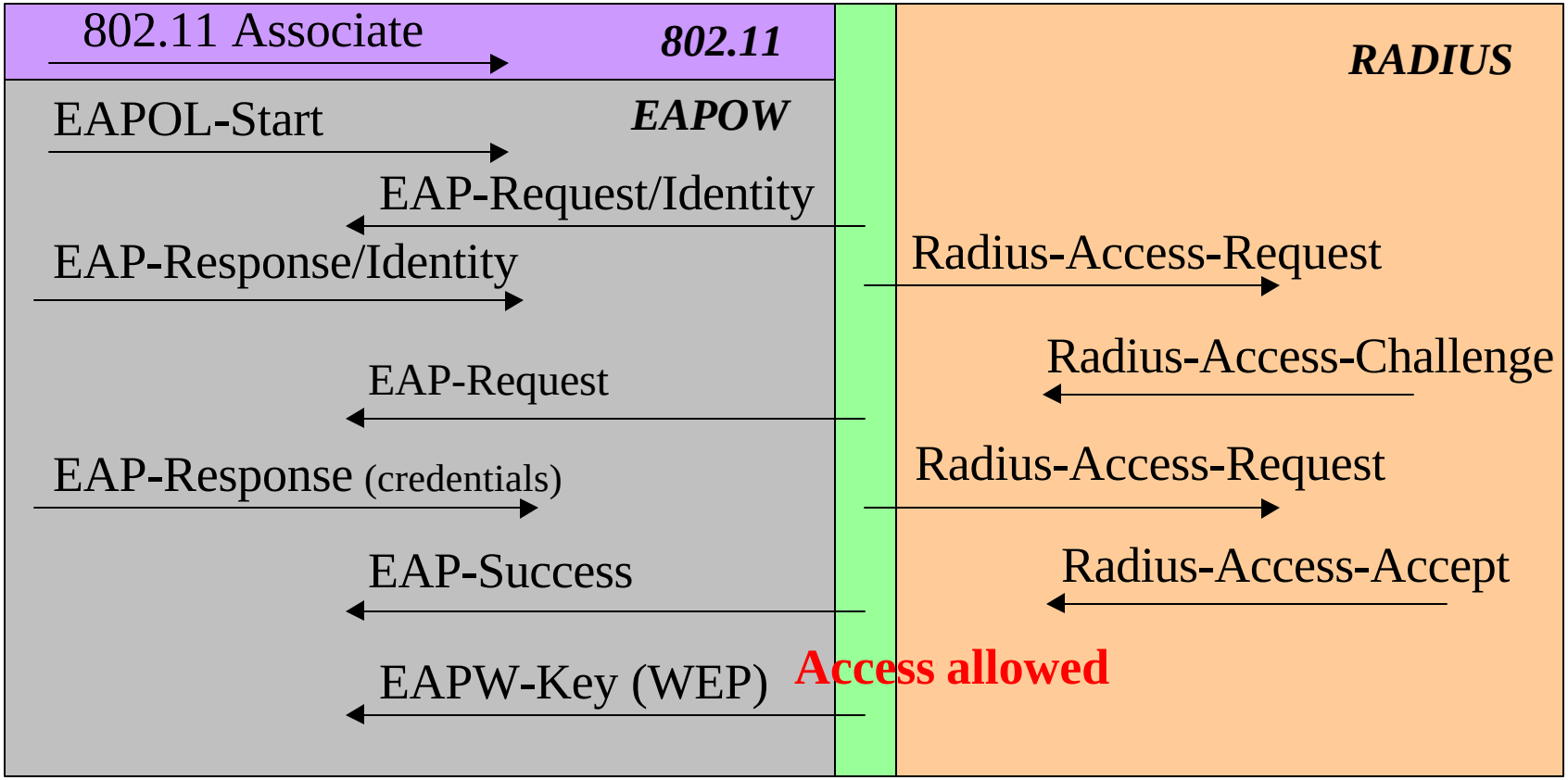
- How can EAPOL be used to derive per-Station unicast session keys?
  - Can use any EAP method supporting secure dynamic key derivation
    - EAP-TLS (RFC 2716)
    - EAP-GSS
    - Security Dynamics
    - Other
  - Keys derived on client and the RADIUS server
  - RADIUS server transmits key to access point
    - RADIUS attribute encrypted on a hop-by-hop basis using shared secret shared by RADIUS client and server
  - Unicast keys can be used to encrypt subsequent traffic, including EAPOW-key packet (for carrying multicast/global keys)
- Per-Station unicast session keys not required
  - If only multicast/global keys are supported, then session key is only used to encrypt the multicast/global key

802.1X and Multicast/Global Keys

- How can EAPOL transfer multicast/global keys?
  - A new EAPOL packet type can be defined for use in transporting multicast/global keys: EAPOW-Key
  - EAPOW-Key packet type used to transmit one or more keys from access point to client
  - EAPOW-Key packets only sent after EAPOW authentication succeeds
  - EAPOW-Key packets are encrypted using derived per-STA session key

802.1X On 802.11





Re-authentication

- Access points are allowed to force clients to re-associate at any time
  - Default is 60 minutes
  - The client responses transparently to the user
- Access point sends WEP global key to client using 802.lX
  - EAPOW-Key message used to send global key

Roaming

- Process (no pre-authentication)
  - 802.11 Re-association
  - 802.1X will re-authenticate but network access will be denied during re-authentication
- Optional support for fast handoff
  - Inter-access point protocol
    - Handoff per client keys
    - Use EAPOW-Key to update shared key
  - Shared key pre-authentication
    - Shared authentication using global WEP key
    - If succeeds then allow immediate access to network
      - i.e. 802.1X is put immediately into the authenticated state

“Unauthenticated” VLAN Support

- Potential extension to IEEE 802.1X
- Designed to enable access to a registration server, enrollment server, etc. prior to authentication
- EAP-Notification message can inform user of location of server to take credit card, enroll user, etc. prior to obtaining network access.

802.1X and Ad-Hoc Networking

- What is ad-hoc networking?
  - Station communicating directly with other stations
- How does ad-hoc networking work with 802.lX?
  - Both Stations initiate EAPOL conversation
  - All stations authenticate with each other
    - Otherwise mutual authentication required and algorithm to select authenticator
  - RADIUS not used in ad-hoc mode
    - Typically implies that user credentials are stored on Stations

Key Management for Ad-Hoc Networking

- Requirements
  - Password-based mutual authentication
  - Secure key generation
- Evaluation of existing EAP methods
  - EAP-TLS: supports mutual authentication, keying, but assumes both participants have a certificate
  - EAP-GSS: supports mutual authentication, assumes "server" side is in contact with KDC
- 802.1X will work in adhoc mode if required
  - Shared key is better for some user scenarios
  - May need new EAP method for this purpose

How 802.1X Addresses 802.11 Security Issues

- User Identification & Strong authentication
- Dynamic key derivation
- Mutual authentication
- Per-packet authentication
- Dictionary attack precautions

Summary of 802.11/802.1X Vulnerabilities

	802.11 w/per packet IV	**802.1X, TLS & Key change**	**802.1X, TLS, Key Change, MIC**
Global keying	vulnerable	fixed	fixed
Impersonation	vulnerable	fixed	fixed
NIC theft	vulnerable	fixed	fixed
Brute force attack (40 bit key)	128-bit	128-bit	128-bit
Rogue Servers	vulnerable	fixed	fixed
Packet spoofing	vulnerable	vulnerable	fixed
Disassociation spoofing	vulnerable	vulnerable	fixed
Passive monitoring	MAC	Identity	Identity
Dictionary attacks	vulnerable	fixed	fixed

Summary

- IEEE 802.1X offers solutions to 802.11 deployment issues
  - User identification
  - Centralized user management
  - Key management
- Minimal changes required to 802.11 specification
  - Additional MIB parameters for 802.1X/802.11 configuration
- Implementation requirements
  - Support for dynamically derived WEP keys + mutual authentication
  - Support for ad-hoc networking
  - Access-Point functions as RADIUS client
    - Requires support for RFC 2138, 2139, draft-ietf-radius-ext-07.txt
  - Access-Point functions as IEEE 802.1X authenticator PAE
- Addresses most WEP security vulnerabilities

Call to Action

- 802.1X
  - Add changes required for 802.11
    - Messages sent to destination MAC address for 802.11
    - Add EAPOW-Key message
- 802.11
  - Adopt 802.1X as an enhanced authentication and key management method
  - Enable appropriate methods supported by 802.1X to be used for 802.11 authentication and key management
  - MAC changes to improve encryption, integrity protection
  - The IAPP work needs to consider security impact re STA mobility between APs.

For More Information

- IEEE 802.1X
  - http://grouper.ieee.org/groups/802/1/pages/802.1x.html
- RADIUS
  - http://www.ietf.org/rfc/rfc2138.txt
  - http://www.ietf.org/rfc/rfc2139.txt
  - http://www.ietf.org/rfc/rfc2548.txt
  - http://www.ietf.org/internet-drafts/draft-ietf-radius-radius-v2-06.txt
  - http://www.ietf.org/internet-drafts/draft-ietf-radius-accounting-v2-05.txt
  - http://www.ietf.org/internet-drafts/draft-ietf-radius-ext-07.txt
  - http://www.ietf.org/internet-drafts/draft-ietf-radius-tunnel-auth-09.txt
  - http://www.ietf.org/internet-drafts/draft-ietf-radius-tunnel-acct-05.txt
- EAP
  - http://www.ietf.org/rfc/rfc2284.txt
  - http://www.ietf.org/rfc/rfc2716.txt

Simplified Insecure Adhoc Support

- Simple, insecure adhoc networking sometimes desirable
  - Children playing games
  - Need “plug and go” solution without security complications
  - Not appropriate in business situations
- How can this be handled with 802.1X?
  - Clients assume network is un-authenticated
    - An authenticated network will drop packets
  - Clients drop received EAP-Start messages
    - Clients think they are connected to a non-authenticated network
    - Adhoc networking just works.

Why Not Incorporate 802.1X into 802.11 authentication?

- Possible to add 802.1X support in 802.11 authentication phase
  - Requires additional authentication type for EAP
  - Requires additional of new key management functionality in 802.11
- Likely to result in duplication of effort
  - Supplicants supporting 802.1X need duplicate code for 802.11 EAP
  - Supplicant operating system sees 802.11 as 802.3
    - Requires encapsulation/decapsulation in NIC driver to maintain transparency
- Large changes required to 802.11 state machine
  - 802.1X state machine needs to be merged with 802.11 state machine
- No additional security over 802.1X over 802.11 approach
  - Associate/disassociate not encrypted or integrity protected so no additional security provided by doing EAP w/key derivation prior to 802.11 Associate
- Un-authenticated VLANs cannot be supported
  - Choice either authenticated or unauthenticated