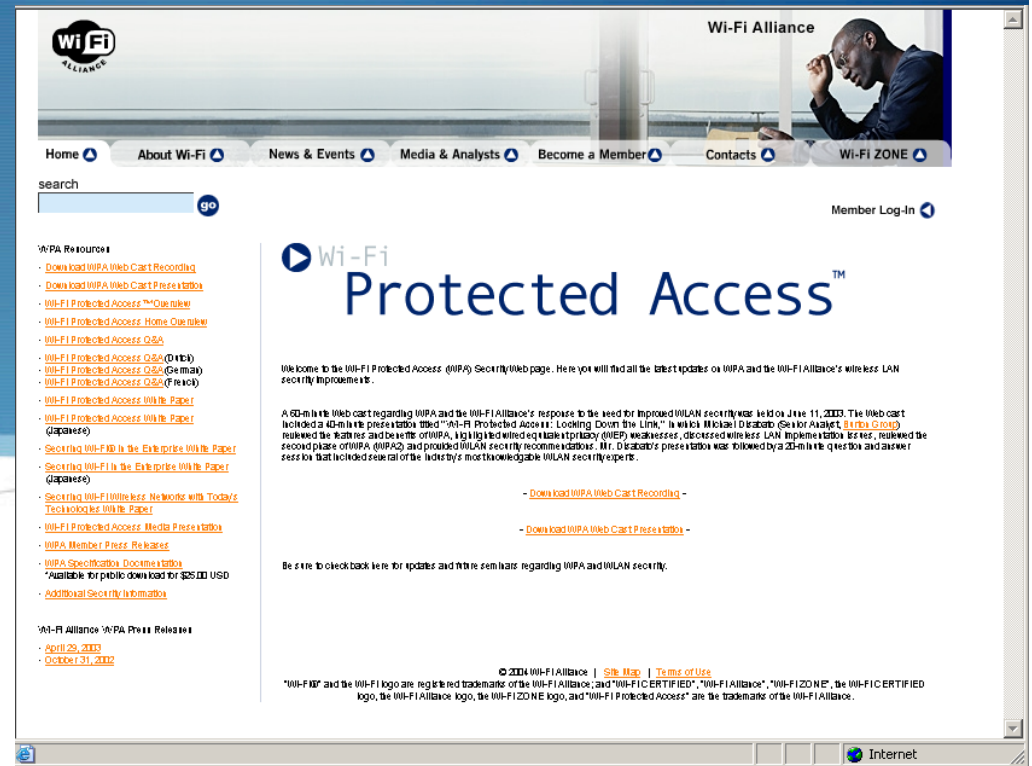


Wi-Fi WPA Presentation



Wi-Fi WPA Presentation

http://www.wifialliance.org/opensection/protected_access.asp



- Welcome to the Wi-Fi Protected Access (WPA) Security Web page. Here you will find all the latest updates on WPA and the Wi-Fi Alliance's wireless LAN security improvements.
- A 60-minute Web cast regarding WPA and the Wi-Fi Alliance's response to the need for improved WLAN security was held on June 11, 2003. The Web cast included a 40-minute presentation titled "**Wi-Fi Protected Access: Locking Down the Link,**" in which Michael Disabato (Senior Analyst, [Burton Group](#)) reviewed the features and benefits of WPA, highlighted wired equivalent privacy (WEP) weaknesses, discussed wireless LAN implementation issues, reviewed the second phase of WPA (WPA2) and provided WLAN security recommendations. Mr. Disabato's presentation was followed by a 20-minute question and answer session that included several of the industry's most knowledgeable WLAN security experts.

Secure 802.11 WLANs

- ◆ WLAN industry recognized the vulnerabilities of 802.11 authentication and data privacy.
- ◆ Changes were incorporated into the 802.11i draft standard.
- ◆ 802.11i was ratified as a standard on May 2004.
- ◆ Wi-Fi Alliance has put together a subset of the components of 802.11i called Wi-Fi Protected Access (WPA).
- ◆ This part of the presentation explains 802.11i and WPA.

Secure 802.11 WLANs

- ◆ Many mistakenly believe WEP to be the only component to WLAN security.
- ◆ Wireless security consists of four facets:
 1. The **Authentication Framework** – The mechanism that accommodates the authentication algorithm by securely communicating messages between the client, AP, and authentication Server.
 2. The **Authentication Algorithm** – Algorithm that validates the user credentials.
 3. The **Data Privacy Algorithm** – Algorithm that provides data privacy across the wireless medium for data frames.
 4. The **Data Integrity Algorithm** – Algorithm that provides data integrity across the wireless medium to ensure to the receiver that the data frame was not tampered with.

1. The Authentication Framework

- ◆ The authentication framework in 802.11 is the 802.11 authentication management frame.
- ◆ The authentication frame facilitates Open and Shared Key authentication algorithms, yet the frame itself does not possess the ability to authenticate the client.

Frame Format of the Authentication Frame

Frame Control	Duration	DA	SA	BSSID	Sequence Control	Authentication Algorithm Numer Field	Authentication Transaction Sequence Numer Field	Status Code Field	Challenge Text IE (Optional)
---------------	----------	----	----	-------	------------------	--------------------------------------	---	-------------------	------------------------------

1. The Authentication Framework

- ◆ 802.11 is missing some key components:
 - ◆ Centralized, user-based authentication
 - ◆ Dynamic encryption keys
 - ◆ Encryption key management
 - ◆ Mutual Authentication

1. The Authentication Framework

Centralized, user-based authentication

- ◆ Critical for network security
- ◆ **Device-based authentication** such as Open or Shared Key, does not prevent unauthorized users from using authorized devices.
- ◆ Logistical issues as network administrators must rekey all 802.11 APs and clients if:
 - ◆ Lost or stolen devices
 - ◆ Employee termination
- ◆ **Centralized, user-based management** via authentication, authorization, and accounting (AAA) server, such as RADIUS, lets you allow or disallow specific users, regardless of the specific devices they use.

1. The Authentication Framework

Dynamic encryption keys

- ◆ User-based authentication has a positive side effect: user-specific encryption keys.
- ◆ Per-user, dynamic keys relieve the network administrator from having to statically manage keys.
- ◆ Encryption keys are dynamically derived and discarded as the user authenticates and disconnects from the network.

Encryption key management

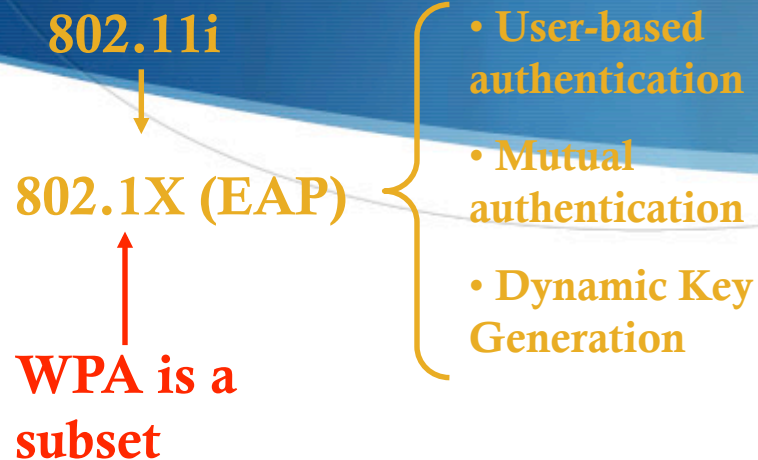
- ◆ Should the need to remove a user from the network, you only need to disable her account to prevent her access.

1. The Authentication Framework

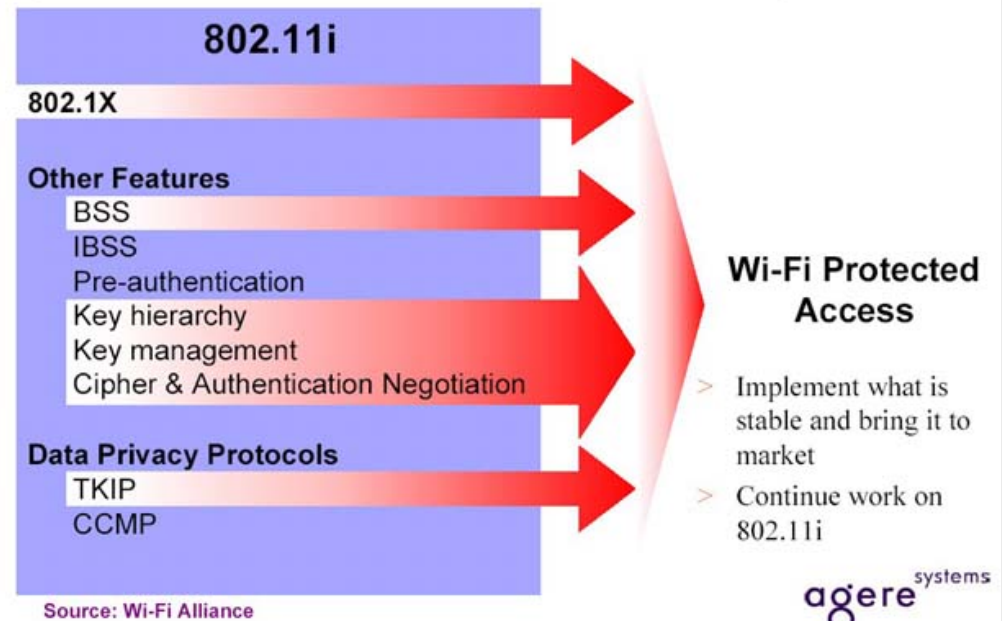
Mutual Authentication

- ◆ Mutual authentication is two-way authentication.
- ◆ Not only does the network authenticate the client, but the client also authenticates the network.
- ◆ In Open and Shared Key authentication, the AP or network authenticates the client.
- ◆ The client does not know for sure that the AP or network is valid because no mechanism is defined in 802.11 to allow the client to authenticate the network.
- ◆ A rogue AP or client posing as a valid AP can subvert the data on the client's machine.

1. The Authentication Framework



WPA is a snapshot of Draft IEEE 802.11i D3.0

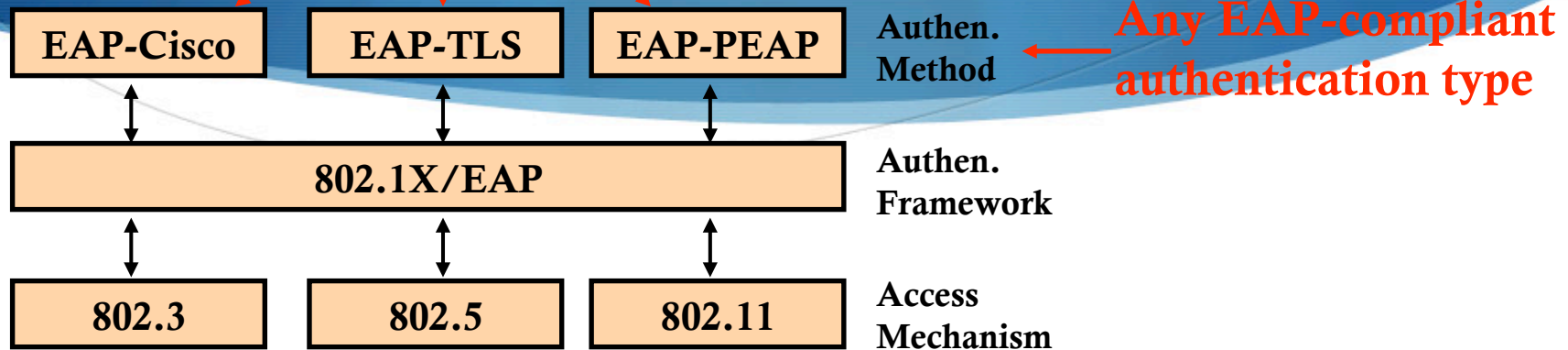


- ◆ IEEE has addressed the shortcomings of 802.11 authentication by incorporating **802.1X authentication framework**.
- ◆ 802.1X itself is an IEEE standard that provides all 802 link layer topologies with extensible authentication, normally seen in higher layers.
- ◆ 802.1X is based on a Point-to-Point (PPP) authentication framework known as Extensible Authentication Protocol (EAP).
- ◆ In oversimplified terms, 802.1X encapsulates EAP messages for use at Layer 2.
- ◆ 802.11i incorporates the 802.1X authentication framework requiring its use for user-based authentication.

1. The Authentication Framework

802.1X

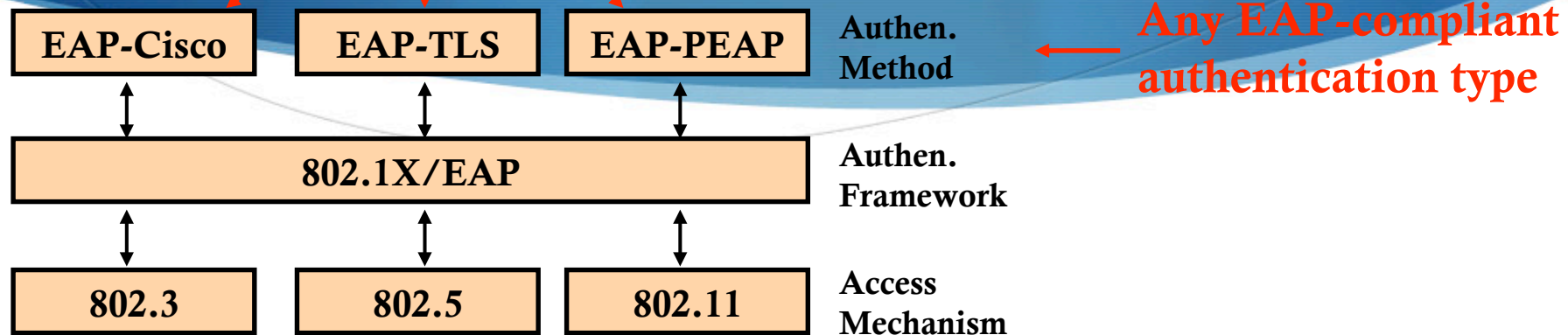
Differing environments



- ♦ EAP (RFC 2284) and 802.1X do **not** mandate the use of any specific authentication algorithm.
- ♦ Network administrator can use any EAP-compliant authentication type for either 802.1X or EAP authentication.
- ♦ The only requirement is that both the 802.11 client (known as the supplicant) and the authentication server support the EAP authentication algorithm.
- ♦ This open and extensible architecture lets you use one authentication framework in differing environments, each environment may use a different authentication type.

1. The Authentication Framework

Differing environments



♦ EAP-TLS

- ♦ EAP-Transport Layer Security
- ♦ Mutual Authentication implementation
- ♦ Used in WPA interoperability testing

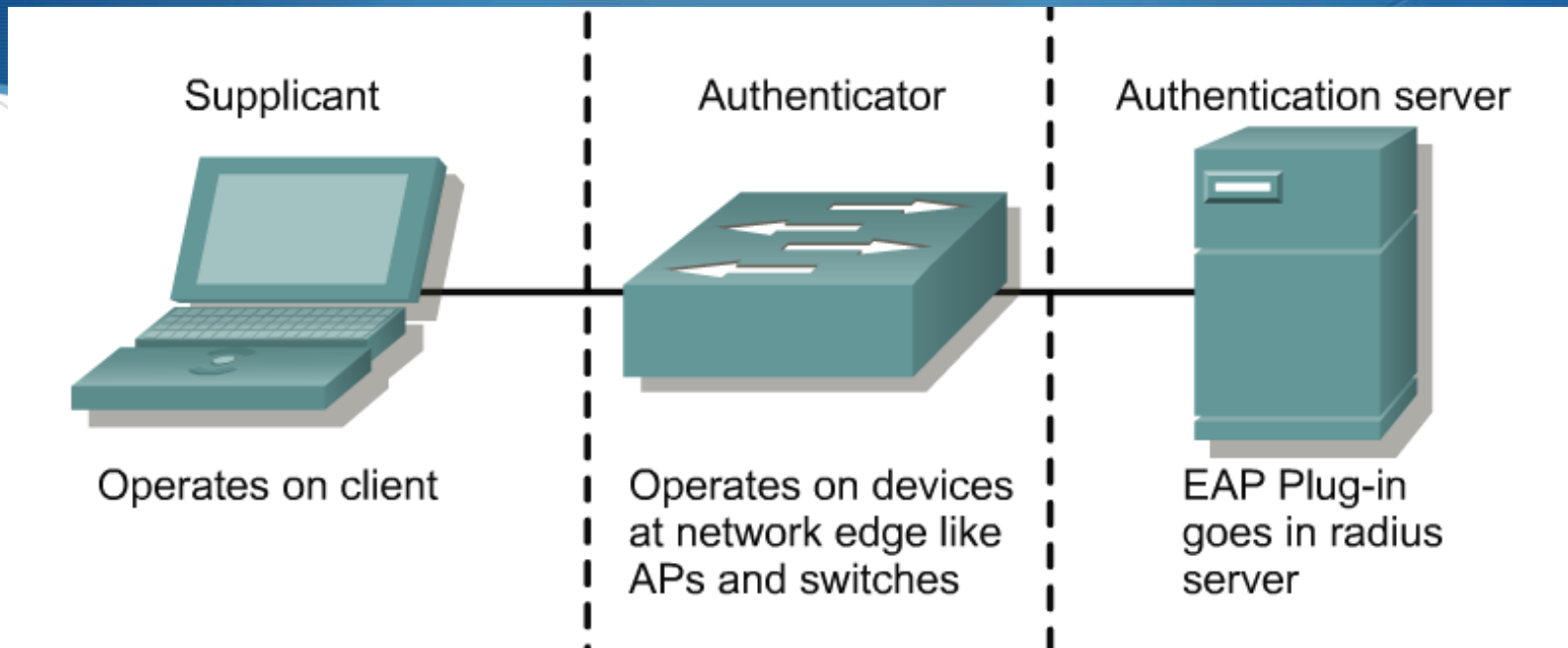
♦ LEAP

- ♦ "Lightweight" EAP
- ♦ Nearly all major OS's supported:
 - ♦ WinXP/2K/NT/ME/98/95/CE, Linux, Mac, DOS

♦ PEAP

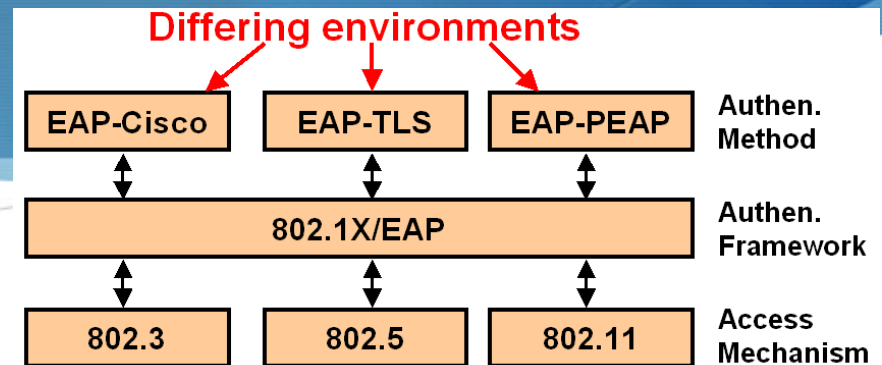
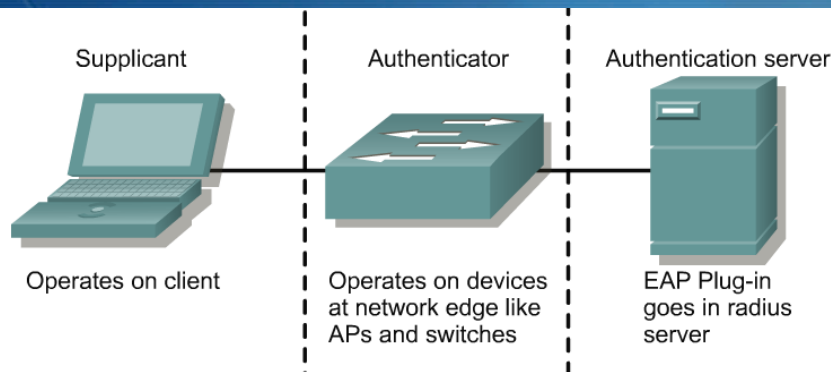
- ♦ "Protected" EAP
- ♦ Uses certificates or One Time Passwords (OTP)
- ♦ Supported by Cisco, Microsoft, & RSA
- ♦ GTC (Cisco) & MSCHAPv2 (Microsoft) versions

1. The Authentication Framework



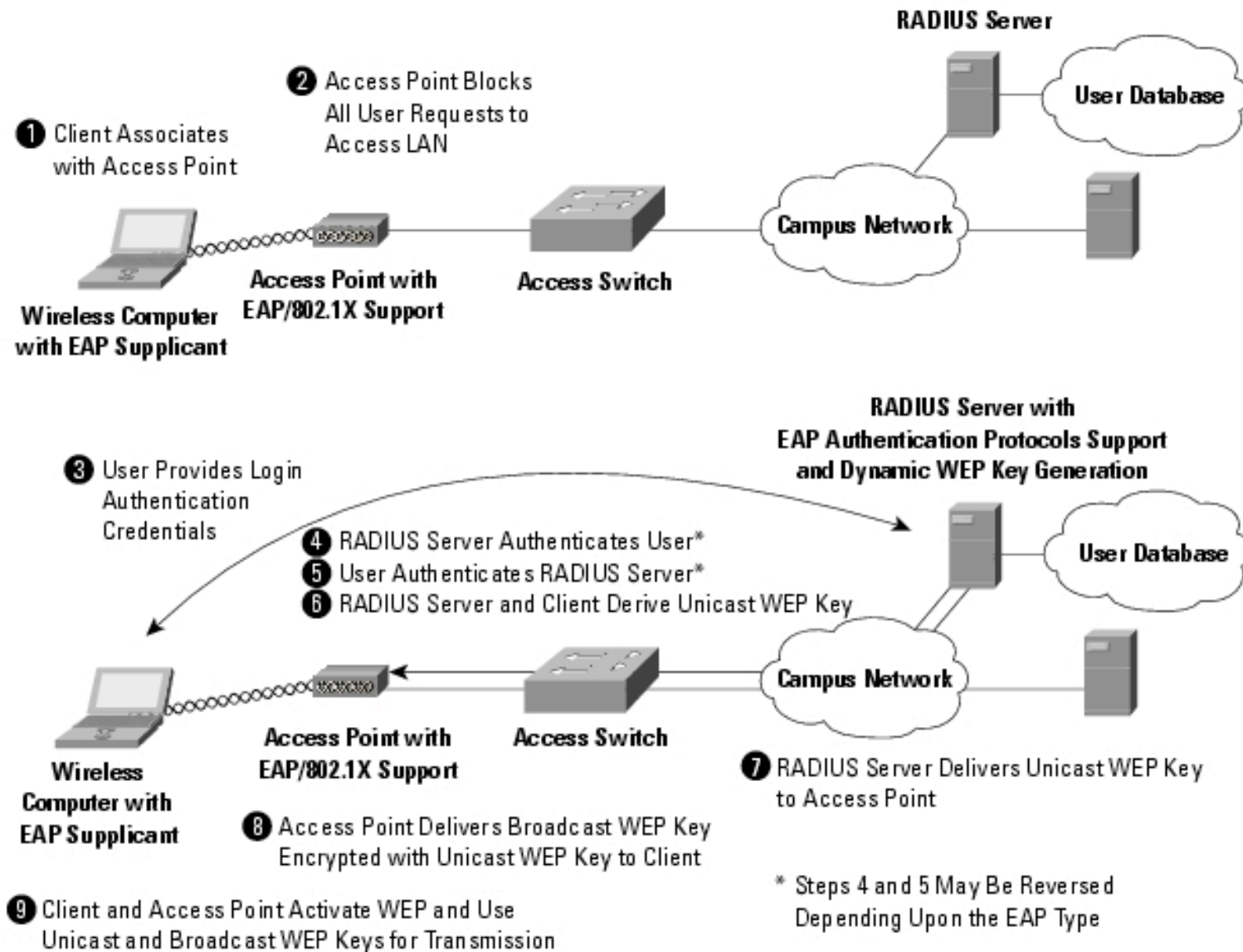
- 802.1X requires three entities
 - Supplicant – Resides on WLAN client
 - Authenticator – Resides on AP
 - Authentication Server – Resides on RADIUS server

2. The Authentication Algorithm

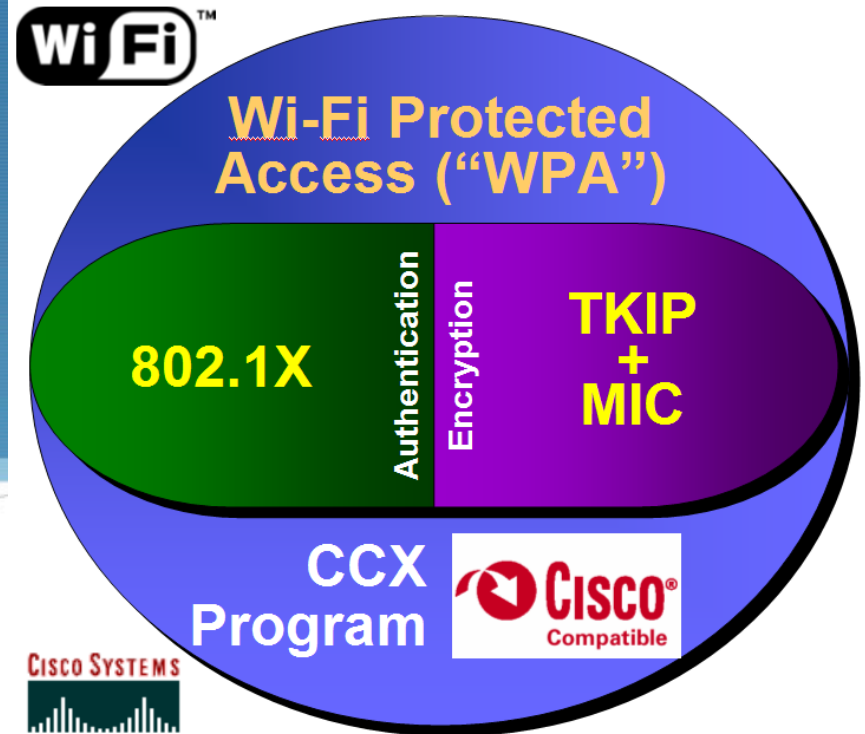


- 802.11i and WPA provide a mechanism for authentication algorithms to communicate between client, AP, and the authentication server, via the 802.1X authentication framework.
- Neither 802.11i nor WPA mandate the use of a specific authentication algorithm, but both recommend the use of an algorithm that supports:
 - mutual authentication
 - dynamic encryption key generation
 - user-based authentication.

EAP Authentication Process

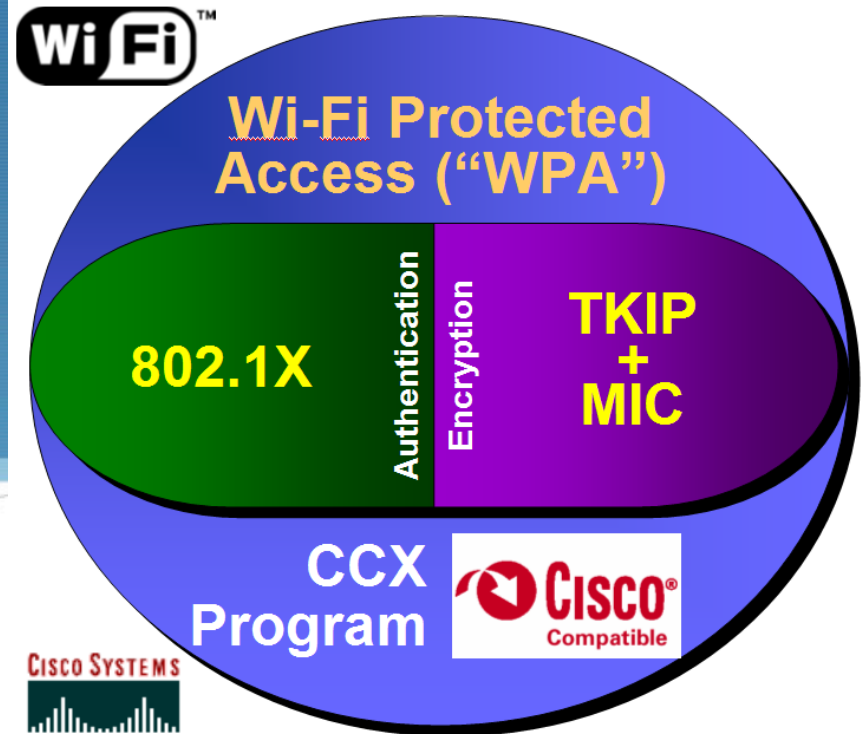


3. Data Privacy



- ◆ The encryption vulnerabilities in WEP present 802.11 vendors and the IEEE with a predicament:
 - ◆ *How can you fix 802.11 encryption without requiring a complete replacement of AP hardware or client NICs?*
- ◆ The IEEE answered this question with **Temporal Key Integrity Protocol (TKIP)** as part of 802.11i (and WPA).
- ◆ TKIP uses many key functions of WEP to maintain client investment of existing 802.11 equipment and infrastructure, but fixes several of the vulnerabilities to provide effect data-frame encryption.

3. Data Privacy

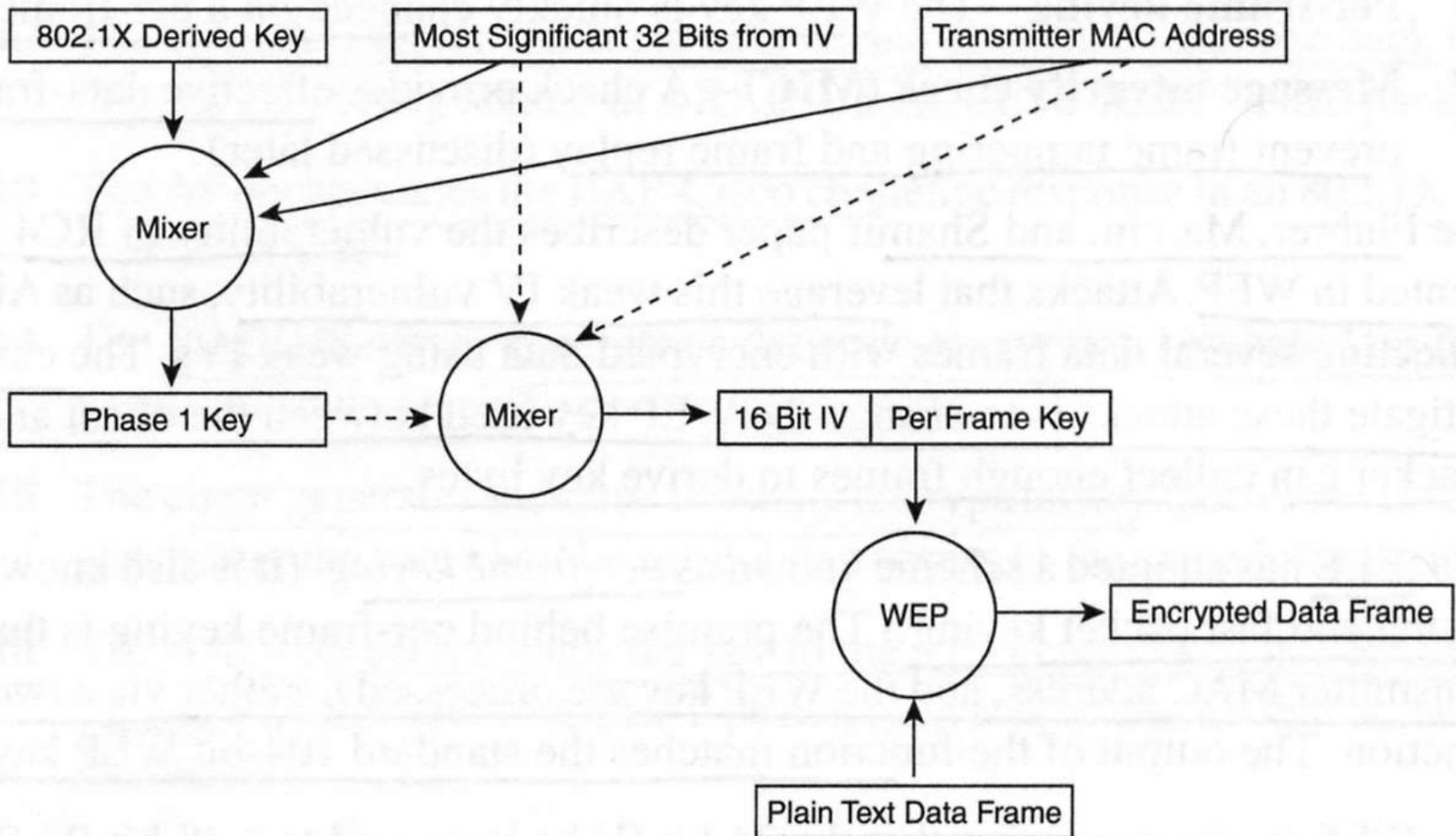


- ◆ The key enhancements with TKIP are:
 - ◆ **Per-frame keying** – The WEP key is quickly changed on a per-frame basis.
 - ◆ **Message integrity check (MIC)** – A check provides effective data-frame integrity to prevent frame tampering and frame replay.
- ◆ Solves statistical attacks such as Aircsnort and the IV vulnerability.
- ◆ Changes WEP key used between client and AP before an attacker can collect enough frames to derive key bytes.

3. Data Privacy

- ◆ The IEEE has adopted a scheme known as per-frame keying (also known as per-packet keying or fast packet keying).
- ◆ The premise behind per-frame keying is that the IV, the transmitter MAC address, and the WEP key are processed together via a two-phase mixing function.
- ◆ The output of the function matches the standard 104-bit WEP key and 24-bit IV.
- ◆ IEEE is also proposing that the 24-bit IV be increased to a 48-bit IV.

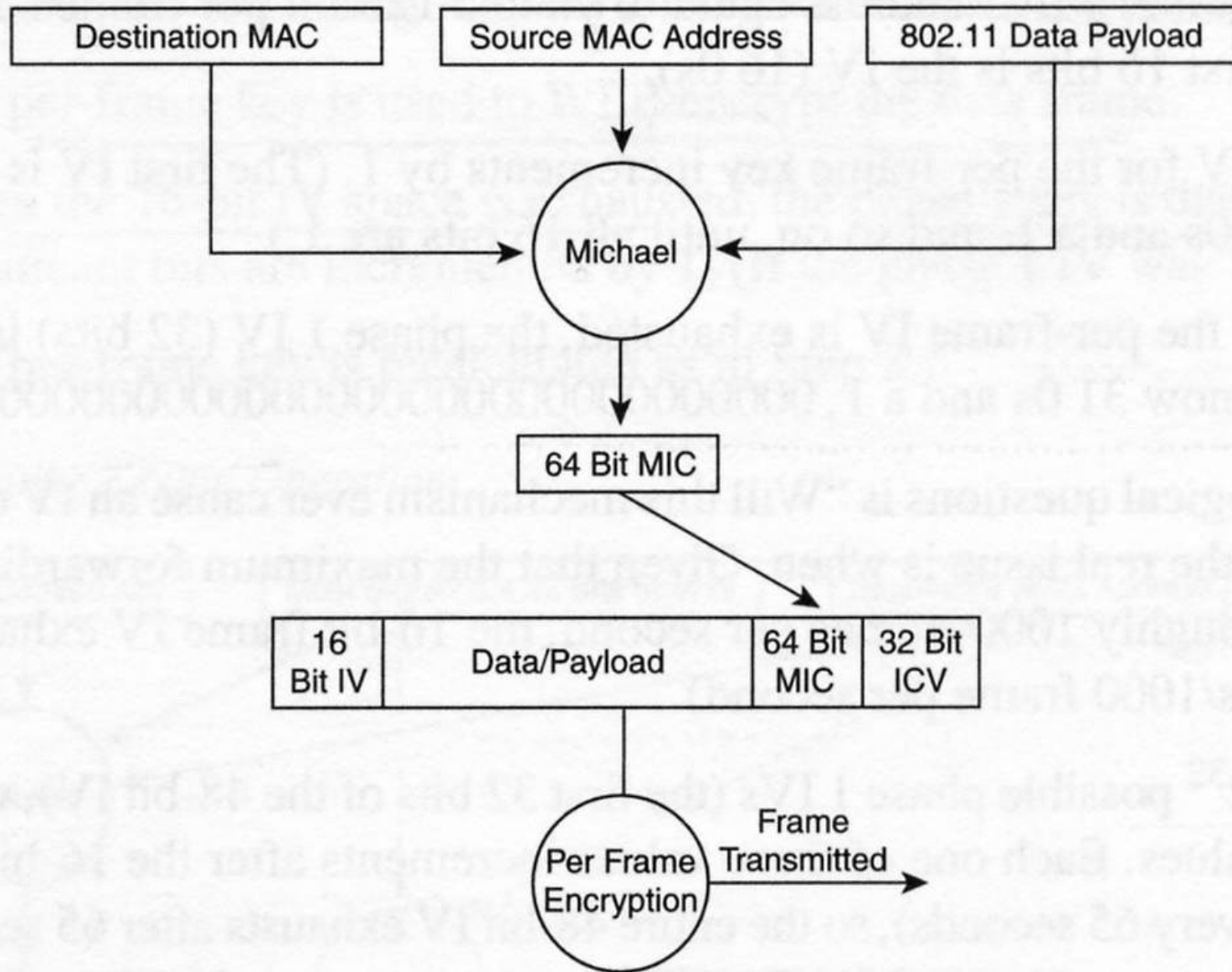
The Per-Frame Keying Operation



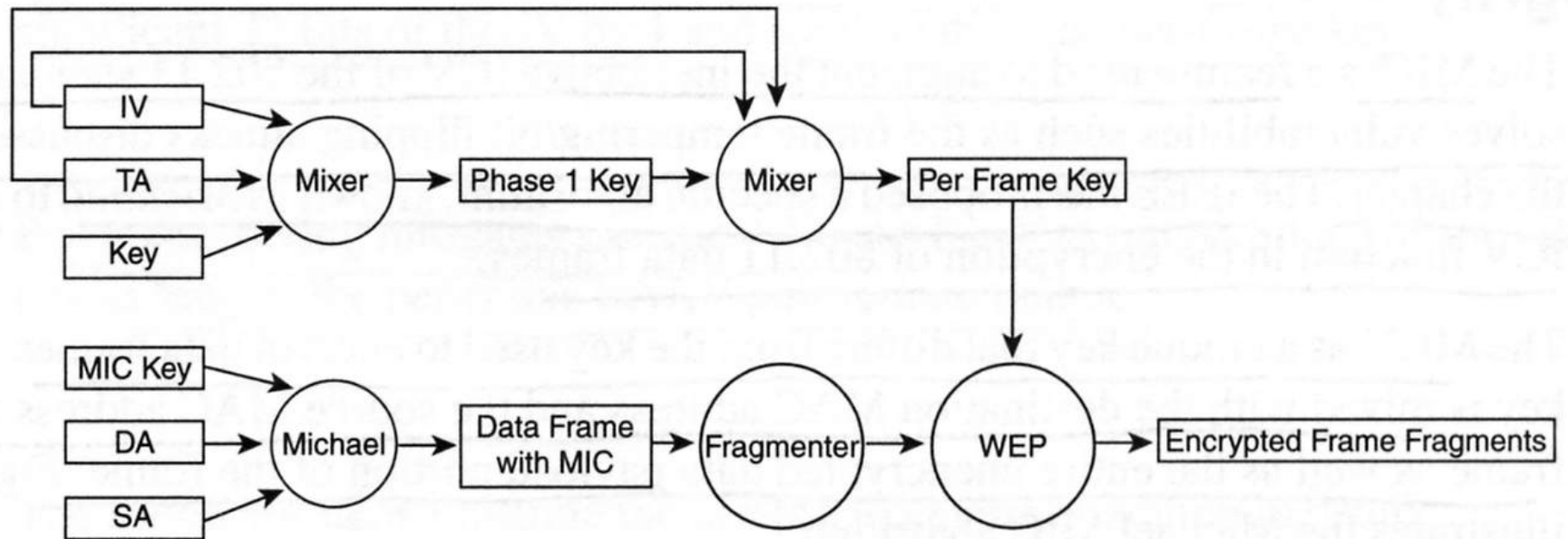
4. Data Integrity

- ◆ The **MIC** is a feature used to augment the ineffective Integrity Check Value (ICV) of 802.11 standard.
- ◆ The MIC solves vulnerabilities such as the frame tampering/bit flipping attacks.
- ◆ The IEEE has proposed a specific algorithm, **Michael**, to augment the ICV function in the encryption of 802.11 data frames.
- ◆ The MIC is a unique key that differs from the key used to encrypt data frames.
- ◆ This unique key is mixed with the destination MAC address and the source MAC address from the frame as well as the entire unencrypted data payload of the frame.

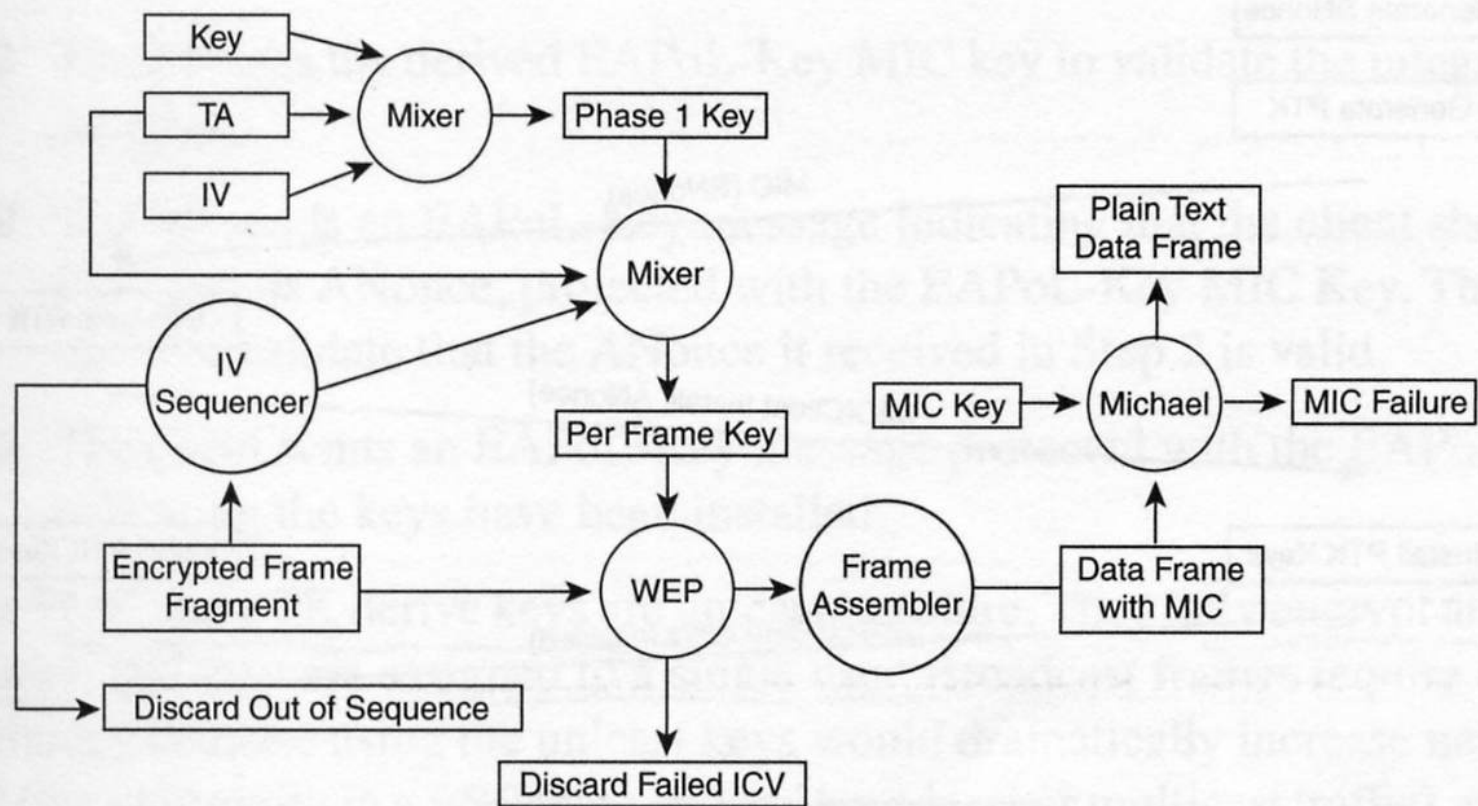
The Michael MIC Algorithm



The TKIP Encryption Process



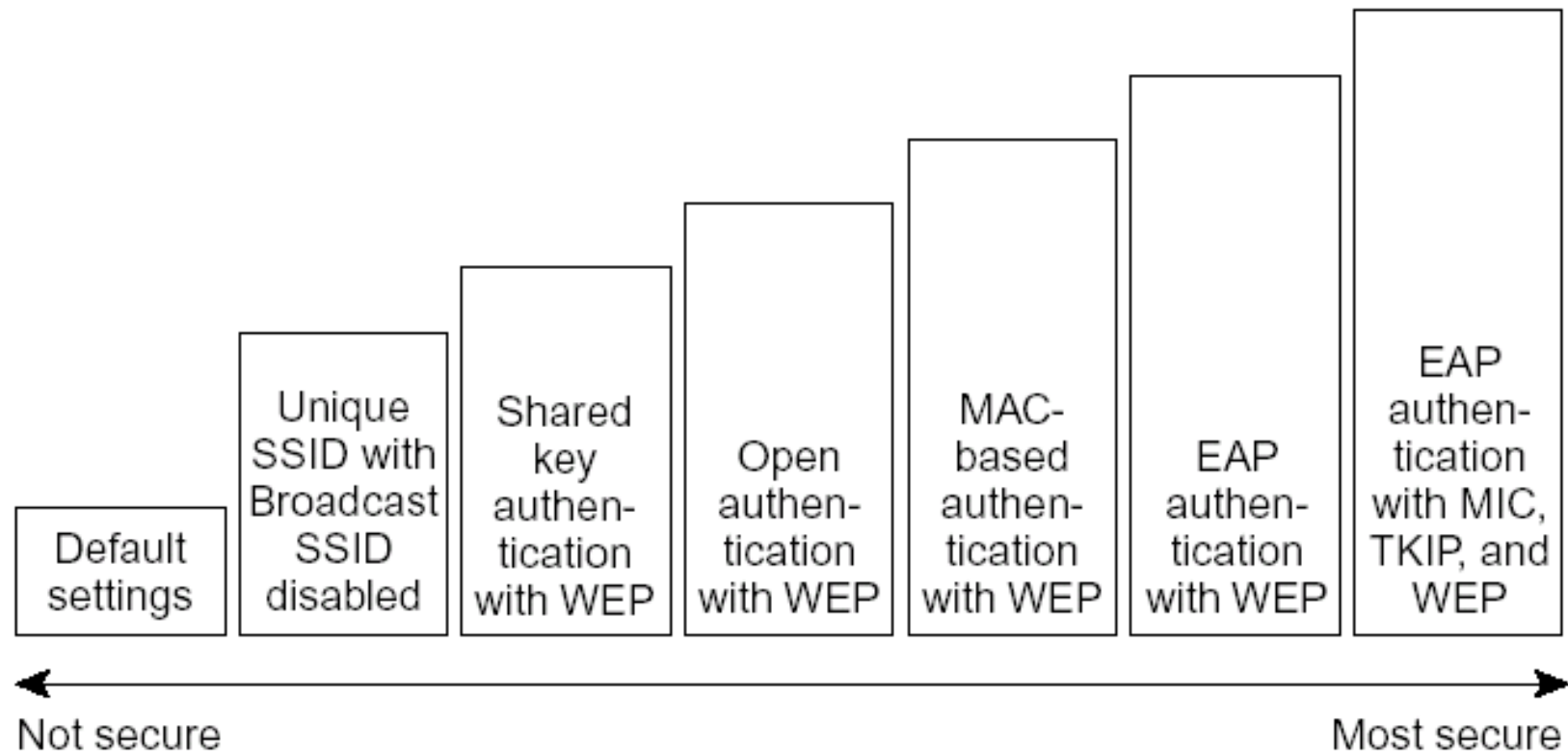
The TKIP Decryption Process



AES

- ◆ WEP encryption and 802.11 authentication are known to be weak.
- ◆ IEEE and WPA are enhancing WEP with TKIP and providing robust authentication options with 802.11Z to make 802.11 based WLANs more secure.
- ◆ At the same time, IEEE is also looking to stronger encryption mechanisms.
- ◆ IEEE has adopted AES to the data-privacy section of the proposed 802.11i standard.
- ◆ WPA does not include support for AES encryption.
- ◆ Later versions of WPA are likely to be released to align with 802.11i for interoperable AES encryption support.
- ◆ AES is the next generation encryption function approved by the National Institute of Standards and Technology (NIST).

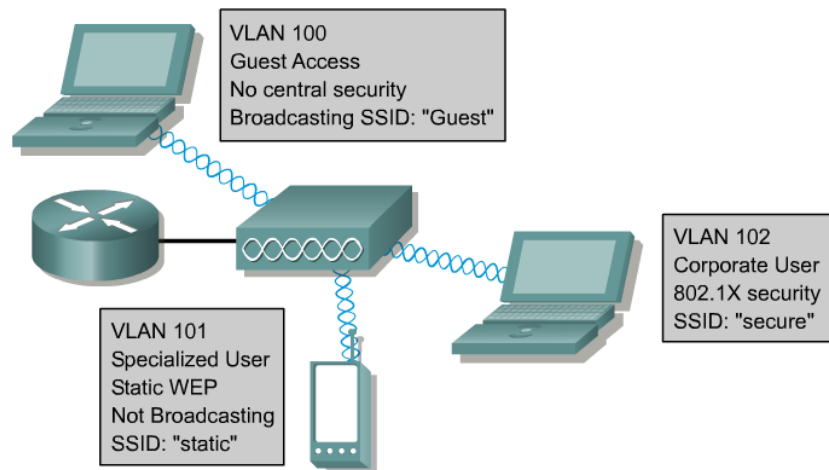
Security Levels



VLANs

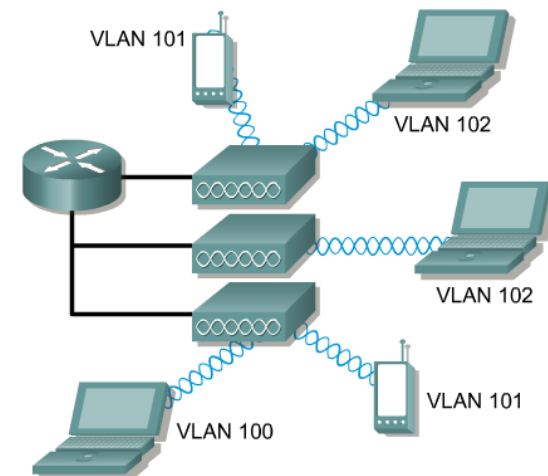


VLANs



VLAN Description

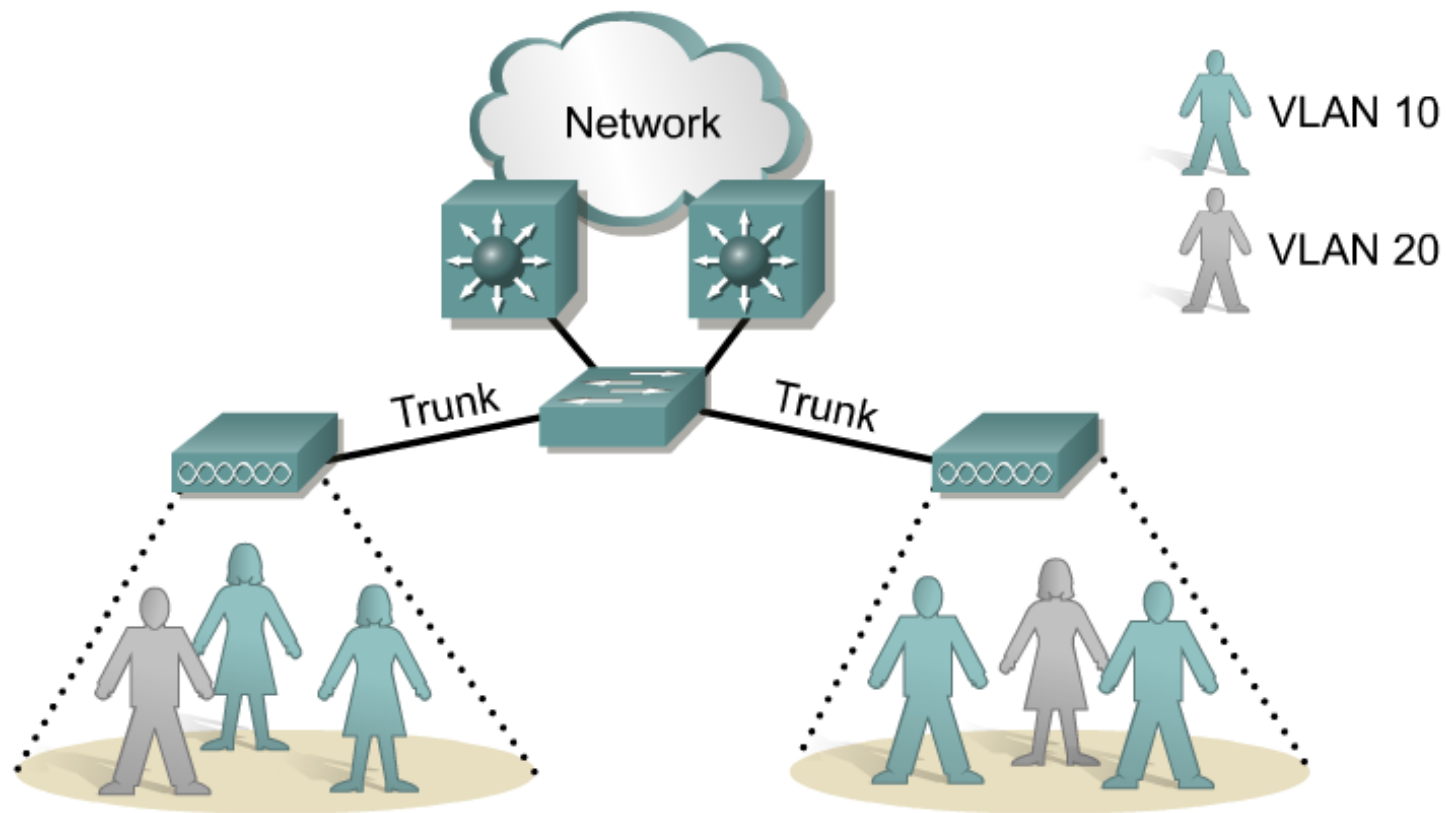
- Multiple SSIDs
- Multiple security types
- Propagates VLANs from switches
- 802.1Q Trunking Protocol



VLAN Description (cont.)

- VLANs propagate across access points
- Unique VLAN numbers
- Access points handle up to 16 VLANs
- Use a router to span across VLANs

VLANs



Enterprise Services: VLANs

- Cisco provides for up to 16 separate VLANs, each with a different SSID
- May be statically or dynamically configured from a RADIUS server, may be mapped to 802.1Q VLANs on switches
- Supports different encryption levels and authentication types on individual segments

Actividad

- ◆ En parejas:
 - ◆ Leer el artículo titulado:
 - ◆ “An Initial Security Analysis of the IEEE 802.1X Standard”
 - ◆ Resumir las ideas principales del artículo (máximo una cuartilla, mínimo media cuartilla)
 - ◆ Indicar los puntos que no hayan entendido
 - ◆ Concluir con su opinión del artículo y los hallazgos encontrados por los autores
- ◆ Fecha límite de entrega: viernes 27 de marzo antes de la hora de clase
- ◆ Formato de entrega: Por correo electrónico a snora@itesm.mx