Authentication

TOPICS

- Objectives
- Legacy Authentication Protocols
- IEEE 802.1X Authentication
- Extensible Authentication Protocol (EAP)
- Authentication Servers

Objectives

- Learn the legacy authentication protocols.
- To identify the purpose and characteristics of 802.1X and EAP.
- Demonstrate the authentication servers: RADIUS/AAA, Kerberos and LDAP used with 802.11 WLANs.
- Understand the various RADIUS Configuration Scenarios.

Legacy Authentication Protocols

- The Legacy Authentication Protocols that are still in use today are:
  - PAP
  - CHAP
  - MS-CHAP
  - MS-CHAPv2

PAP

- Password Authentication Protocol, sometimes abbreviated PAP, is a simple authentication protocol used to authenticate a user to a network access server used for example by internet service providers.
- PAP was originally designed for the use with Point to Point Protocol.
- PAP provides no protection of authentication credentials.

CHAP

- Challenge-Handshake Authentication Protocol (CHAP) authenticates a user or network host to an authenticating entity like an Internet access provider.
- RFC 1994: Challenge Handshake Authentication Protocol (CHAP) defines the protocol.
- CHAP is an authentication scheme used by Point to Point Protocol (PPP) servers to validate the identity of remote clients.
- CHAP periodically verifies the identity of the client by using a three-way handshake, at the time of establishing the initial link.
- The verification is based on a shared secret (such as the client user's password).
  1. After the completion of the link establishment phase, the authenticator sends a "challenge" message to the peer.
  2. The peer responds with a value calculated using a one-way hash function, such as an MD5 checksum hash.
  3. The authenticator checks the response against its own calculation of the expected hash value. If the values match, the authenticator acknowledges the authentication; otherwise it should terminate the connection.
  4. At random intervals the authenticator sends a new challenge to the peer and repeats steps 1 through 3.
- CHAP is not considered the most secure authentication mechanism by today’s standards.

MS-CHAP

- MS-CHAP is the Microsoft version of the Challenge-handshake authentication protocol, CHAP.
- The protocol exist in two versions:
  - MS-CHAPv1 (defined in RFC 2433) and
  - MS-CHAPv2 (defined in RFC 2759).
- Compared with CHAP, MS-CHAP:
  - is enabled by negotiating CHAP Algorithm 0x80 in LCP option 3, Authentication Protocol
  - provides an authenticator-controlled password change mechanism
  - provides an authenticator-controlled authentication retry mechanism
  - defines failure codes returned in the Failure packet message field
- MS-CHAPv2 provides mutual authentication between peers by piggybacking a peer challenge on the Response packet and an authenticator response on the Success packet.

MS-CHAPv2

- MS-CHAPv2 is a proprietary protocol created by Microsoft, was first released with Windows 2000 Professional and Server.
- MS-CHAPv2 improves on MS-CHAP by storing the passwords with a stronger hashing and encryption mechanisms and adding mutual authentication.
- This protocol is commonly used as an internal authentication mechanism in the EAP type known as PEAP.

IEEE 802.1X Authentication

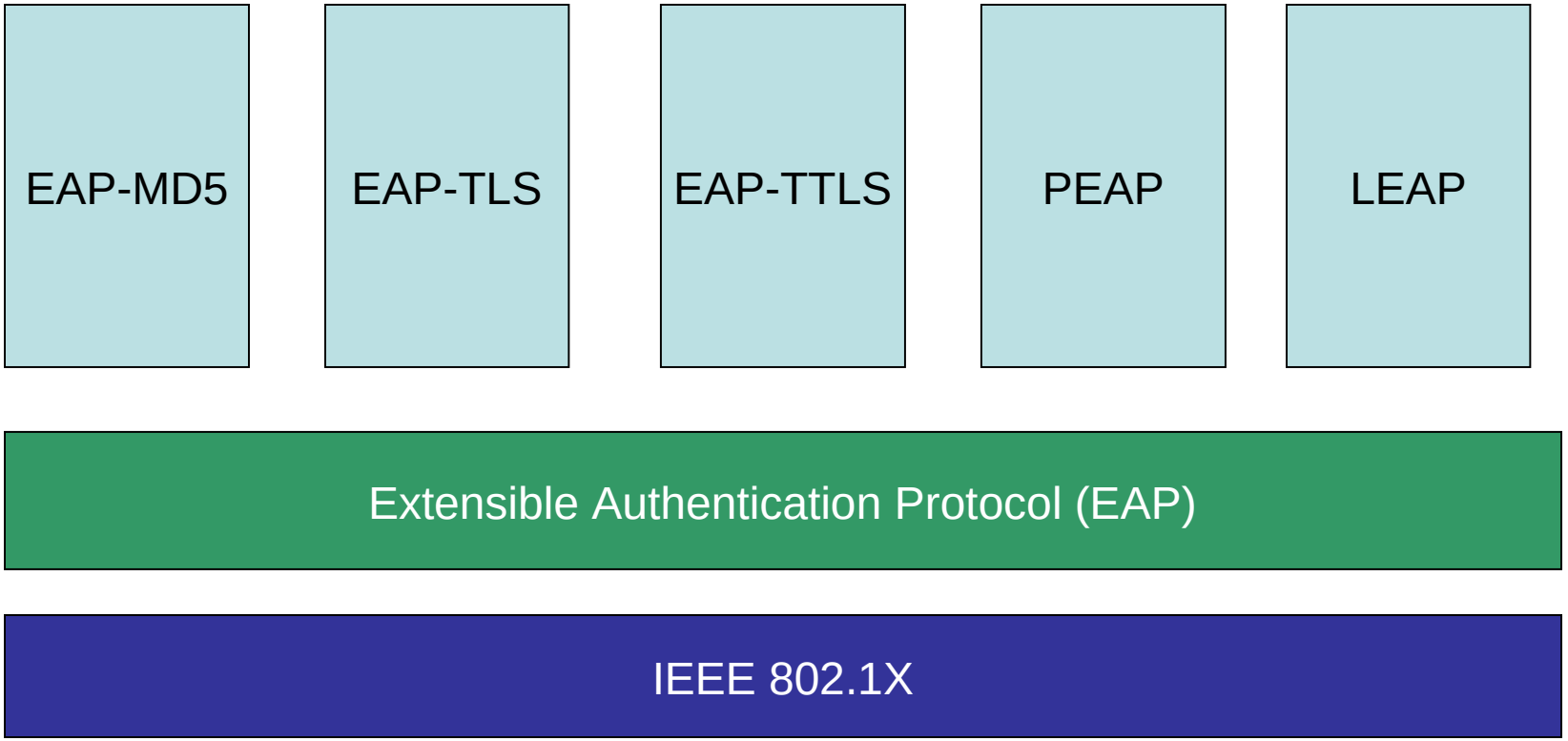
- IEEE 802.1X is an IEEE standard for port-based Network Access Control.
- It provides authentication to devices attached to a LAN port, establishing a point-to-point connection or preventing access from that port if authentication fails.
- 802.1X makes use of EAP to define how authentication messages are to be exchanged between the various network components – Supplicants, Authenticators and Authentication Servers.

Cont…

- The advantages of using 802.1X port-based network authentication include:
  - Multi-Vendor Standard framework for securing the network.
  - Improves security through session based dynamic keying of encryption keys.
  - Standards based message exchange based on EAP.
  - Uses industry standard authentication serves (ex: RADIUS)
  - Uses existing user security information, if necessary.
  - Centralizes management for network access.
  - Supports both wired and wireless networks.

Cont…

- 802.1X Authentication Components:



How 802.1X/EAP works

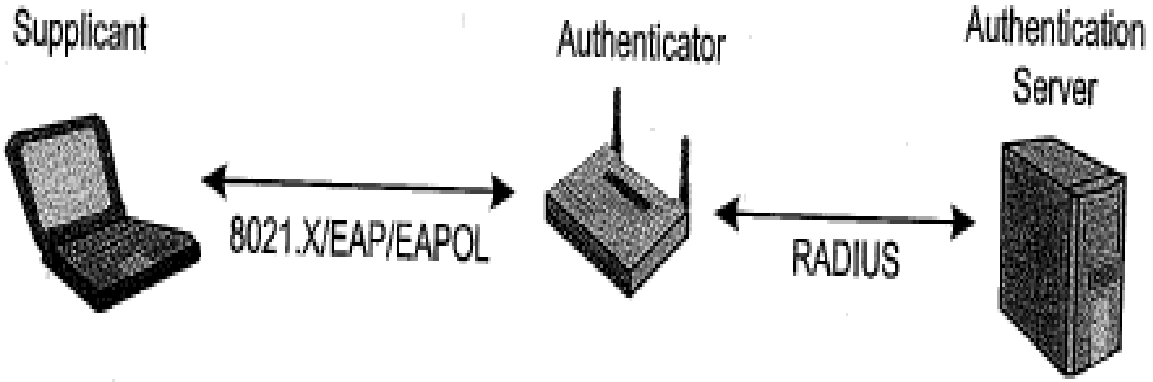
- The more specific functionality of the various EAP types ,the 802.1X supports include:
  - Authentication Roles
  - Controlled and Uncontrolled Ports
  - 802.1X Generic Authentication Flow Framework.

Authentication Roles

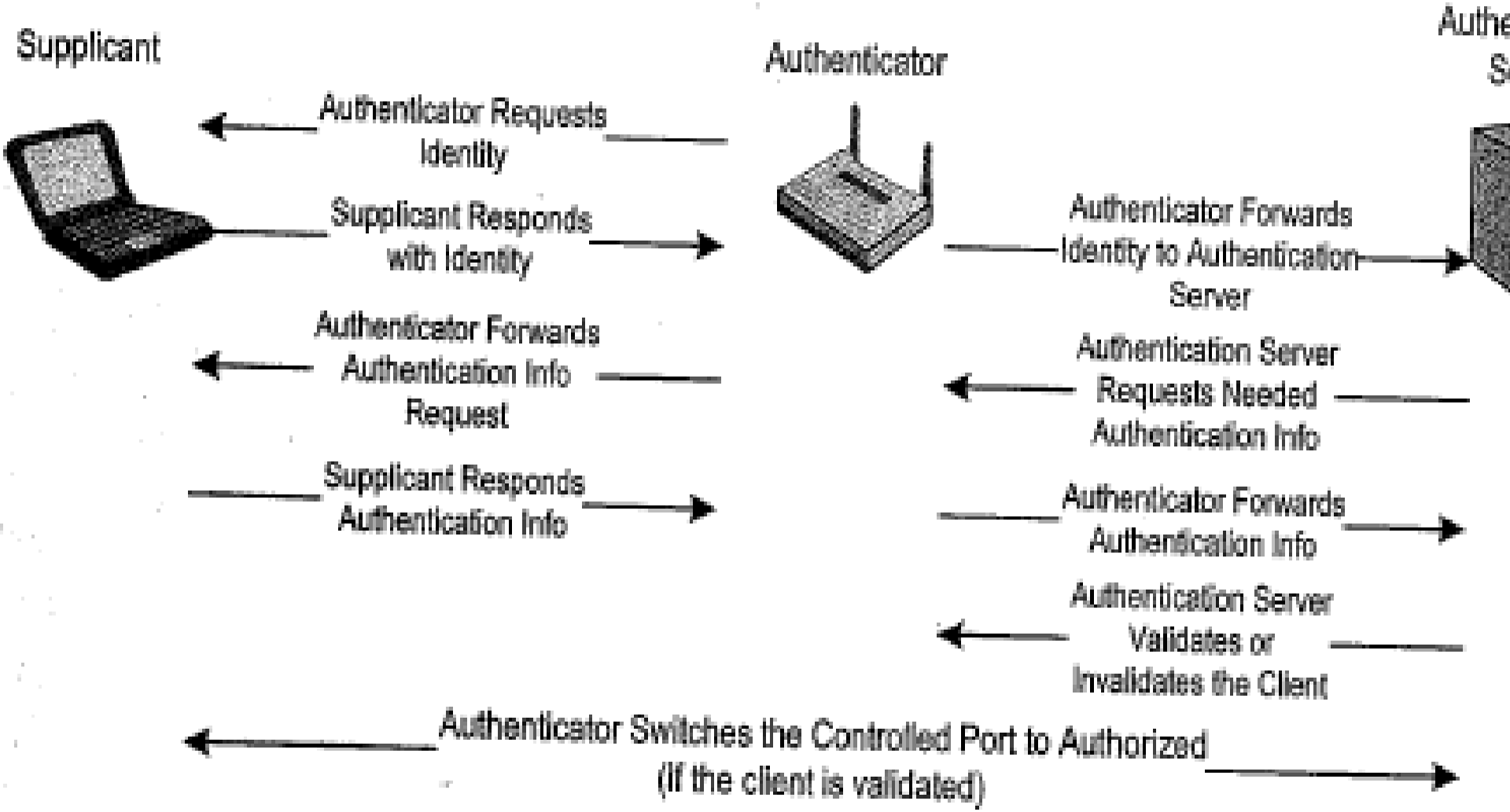
- There are three primary authentication roles in an 802.1X authentication system, that include:
  - Supplicant
  - Authenticator
  - Authentication Server

Cont…

- 802.11X authentication Roles



Generic 802.1X authentication Flow

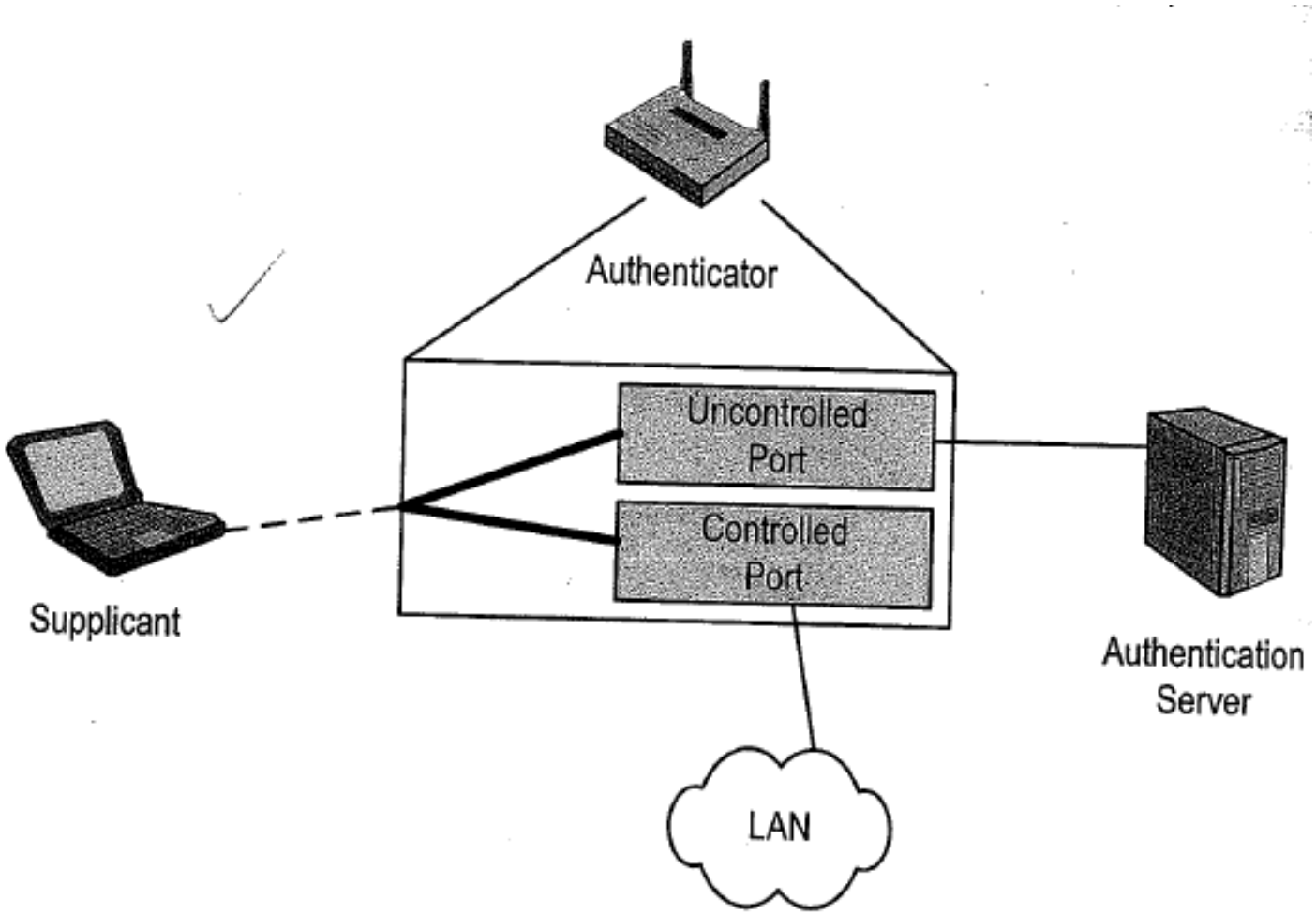


Controlled and Uncontrolled Ports

- Two ports are defined by the 802.1X standard for the purpose of authenticating connected systems, that are:
  - Uncontrolled Port: It is the port that allows communications to pass through the authentication and authorization only.
  - Controlled Port: It is the port that can be used once authentication has completed.

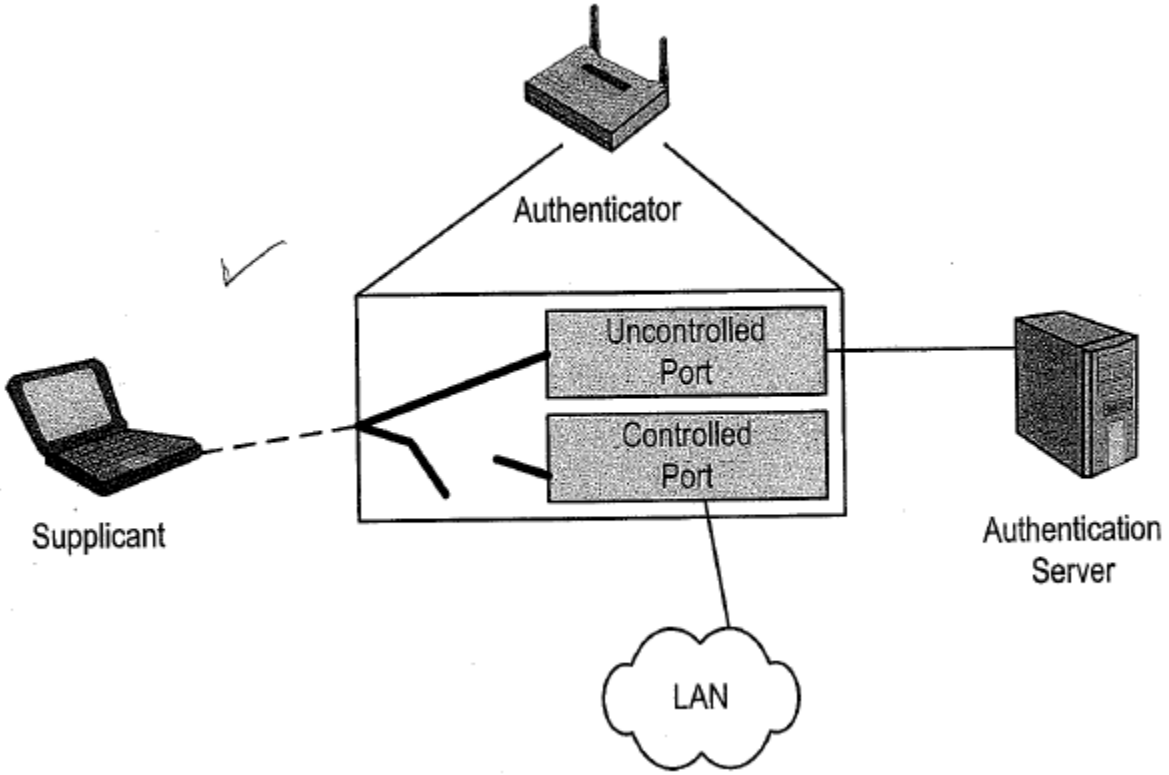
Cont…

- Authorized connection to a wireless ȣ



Cont…

- Unauthorized connection to a wireless 802.1X authenticator (AP)



Extensible Authentication Protocol (EAP)

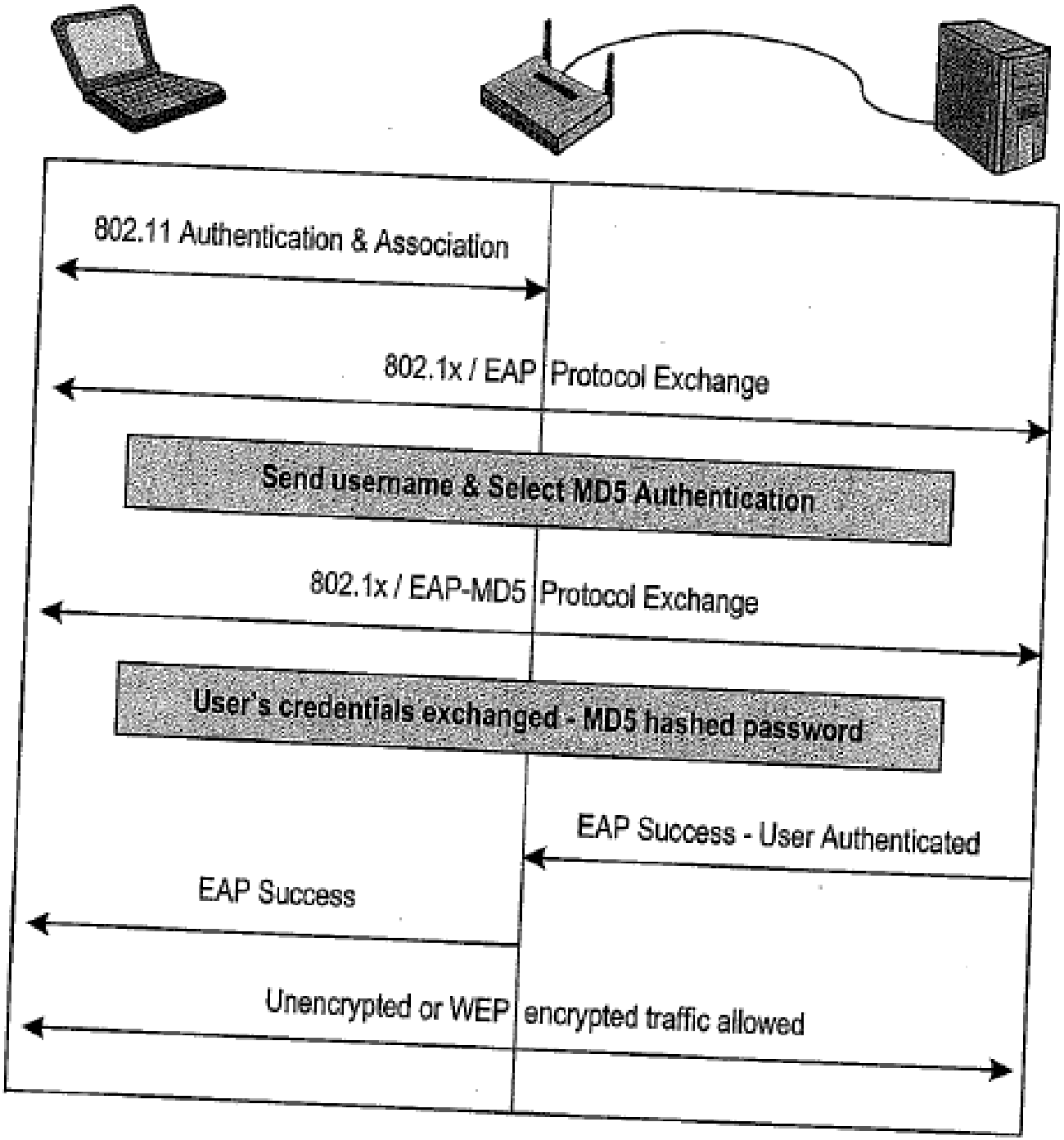
- Extensible Authentication Protocol, or EAP, is a universal authentication framework frequently used in wireless networks and Point-to-Point connections, defined by RFC 3748.
- 802.1X implements EAP over local area networks and the protocol used to carry the EAP messages from the supplicant to the authenticator is EAPOL.

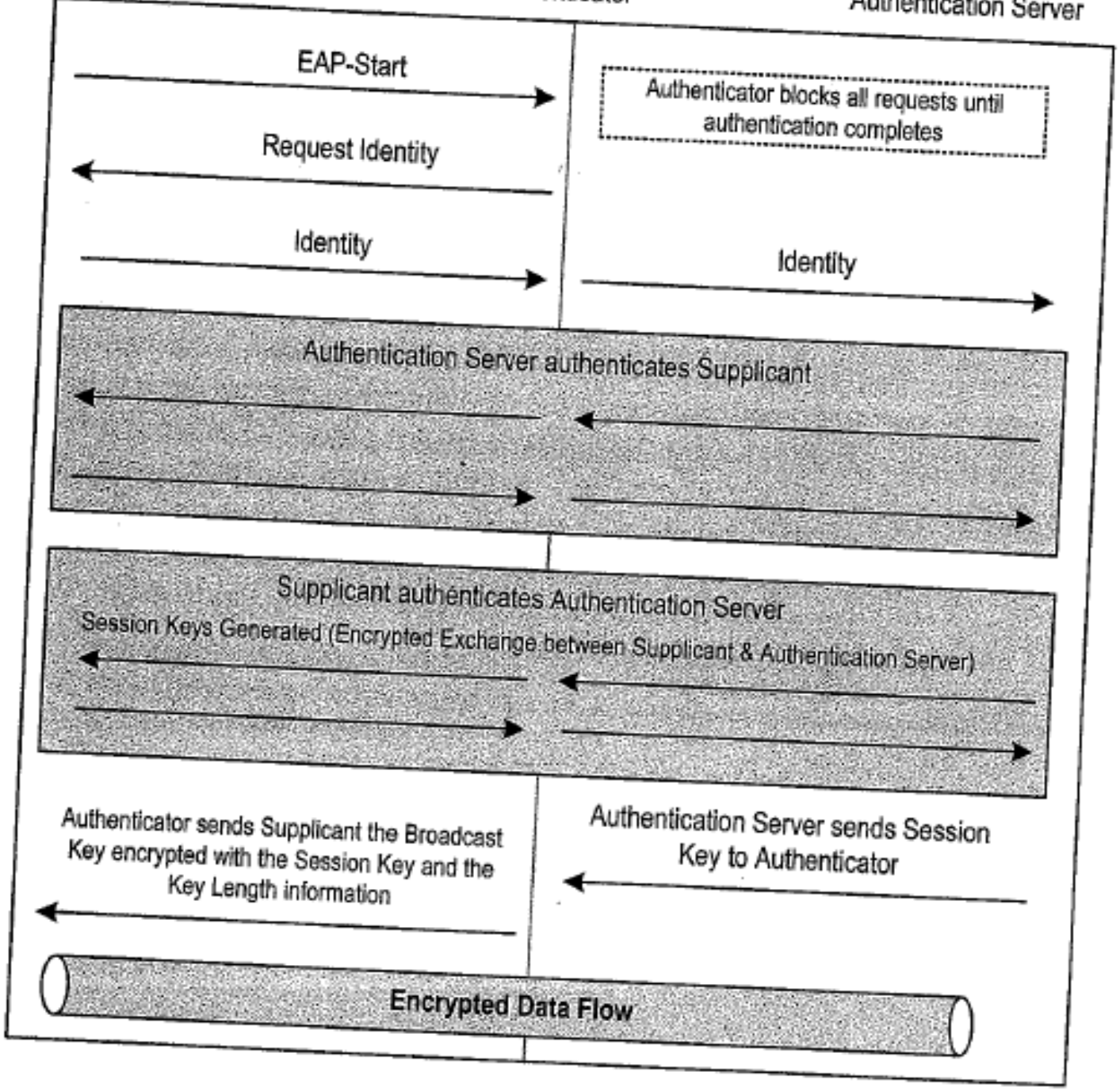
Cont…

- Some of the more common authentication protocols supported by EAP include:
  - EAP-MD5 (Message Digest 5)
  - EAP-TLS (Transport Level Security)
  - EAP-TTLS (Tunneled TLS)
  - EAP-PEAP (Protected EAP Protocol)
  - Cisco LEAP (Lightweight EAP Protocol)

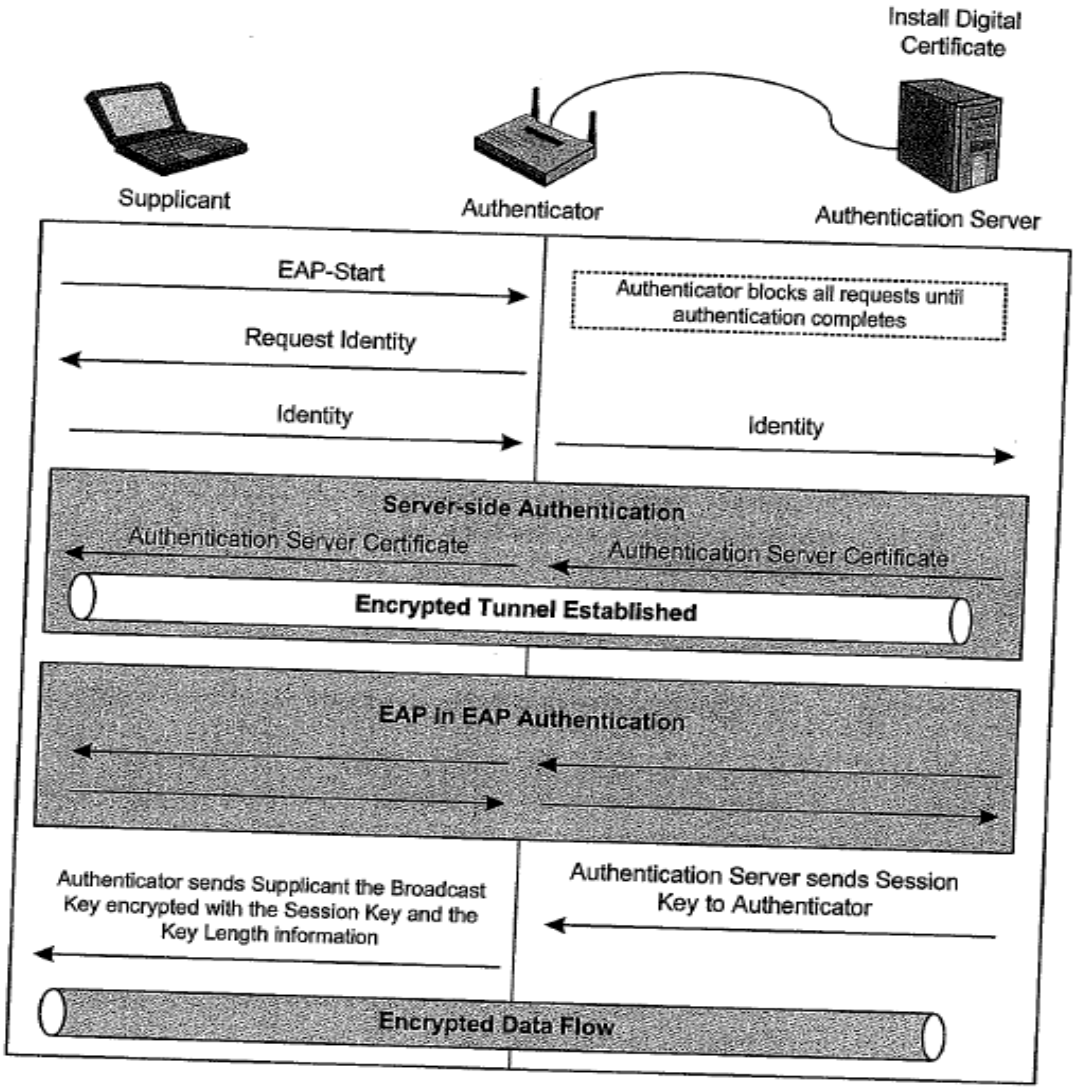
EAP Selection Quick Reference for common Types

	EAP-MD5	LEAP	EAP-TLS	EAP-TTLS	PEAP
Mutual Authentication	No	Yes	Yes	Yes	Yes
Certificates required	No	No	Client/ Server	Server only	Server only
Dynamic Key Generation	No	Yes	Yes	Yes	Yes
Costs and Management overhead	Low	Low	High	Low/ Medium	Low/ Medium
Industry Support	Low	High	Medium	High	High

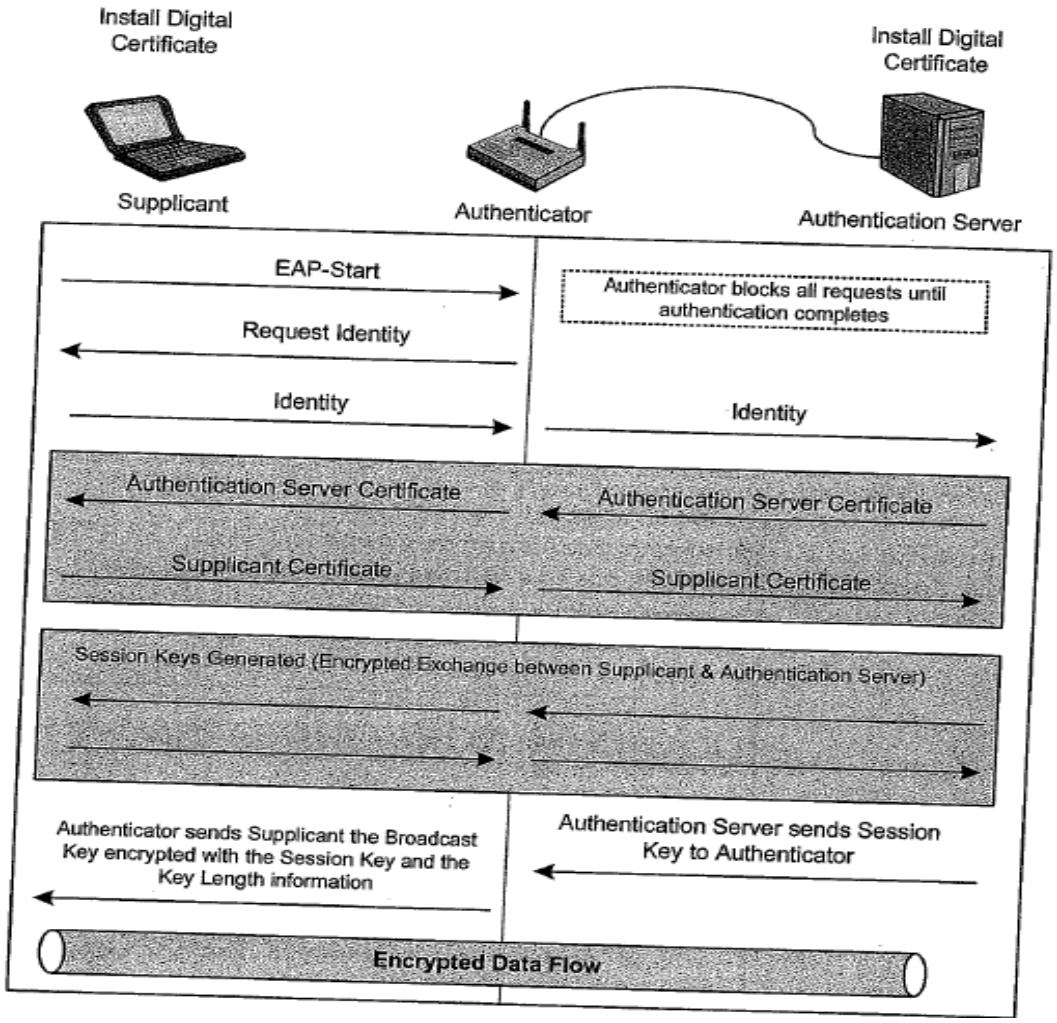

802.11 Authentication & Association
802.1x / EAP Protocol Exchange
Send username & Select MD5 Authentication
802.1x / EAP-MD5 Protocol Exchange
User's credentials exchanged - MD5 hashed password
EAP Success - User Authenticated
EAP Success
Unencrypted or WEP encrypted traffic allowed


Authentication Server
EAP-Start
Authenticator blocks all requests until authentication completes
Request Identity
Identity
Identity
Authentication Server authenticates Supplicant
Supplicant authenticates Authentication Server
Session Keys Generated (Encrypted Exchange between Supplicant & Authentication Server)
Authenticator sends Supplicant the Broadcast Key encrypted with the Session Key and the Key Length information
Authentication Server sends Session Key to Authenticator
Encrypted Data Flow

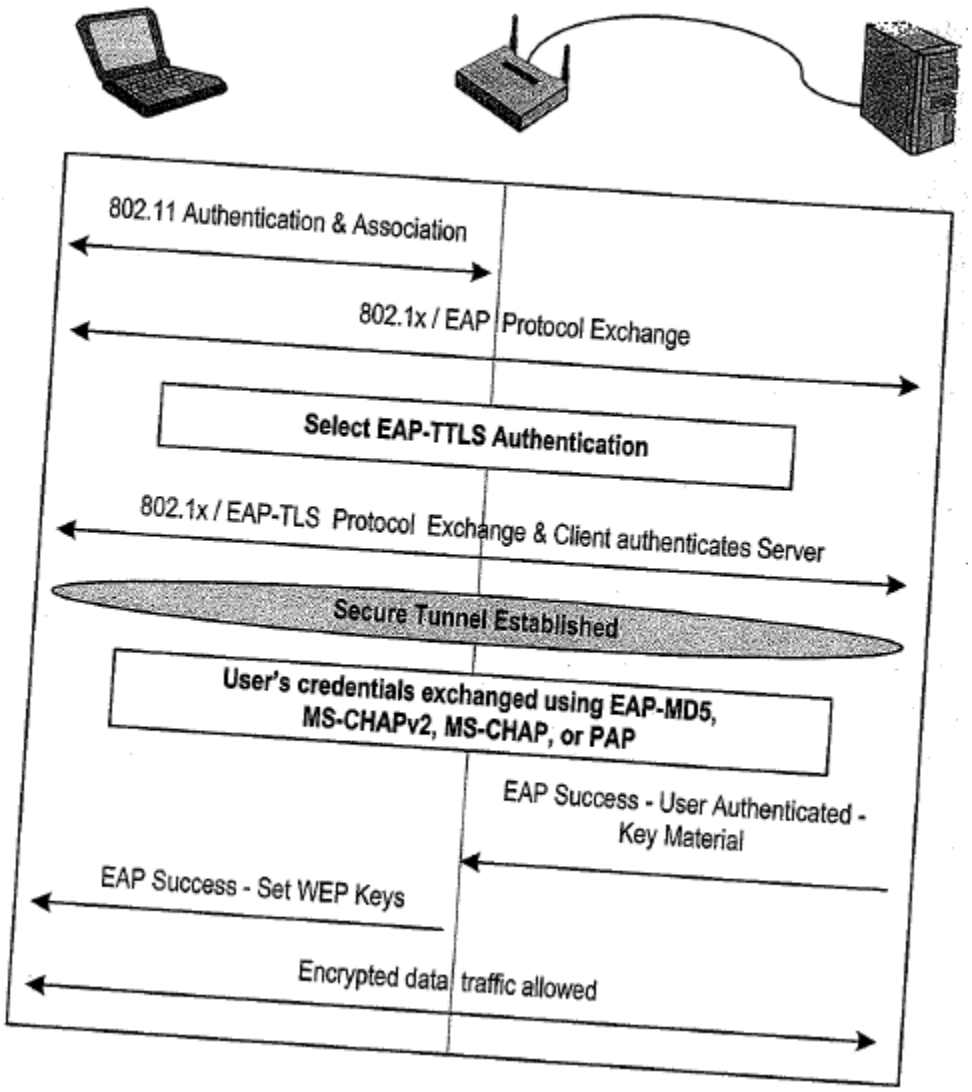
PEAP


Install Digital Certificate
Supplicant
Authenticator
Authentication Server
EAP-Start
Authenticator blocks all requests until authentication completes
Request Identity
Identity
Identity
Server-side Authentication
Authentication Server Certificate
Authentication Server Certificate
Encrypted Tunnel Established
EAP in EAP Authentication
Authenticator sends Supplicant the Broadcast Key encrypted with the Session Key and the Key Length information
Authentication Server sends Session Key to Authenticator
Encrypted Data Flow

EAP-TLS


Install Digital Certificate
Install Digital Certificate
Supplicant
Authenticator
Authentication Server
EAP-Start
Authenticator blocks all requests until authentication completes
Request Identity
Identity
Identity
Authentication Server Certificate
Authentication Server Certificate
Supplicant Certificate
Supplicant Certificate
Session Keys Generated (Encrypted Exchange between Supplicant & Authentication Server)
Authenticator sends Supplicant the Broadcast Key encrypted with the Session Key and the Key Length information
Authentication Server sends Session Key to Authenticator
Encrypted Data Flow

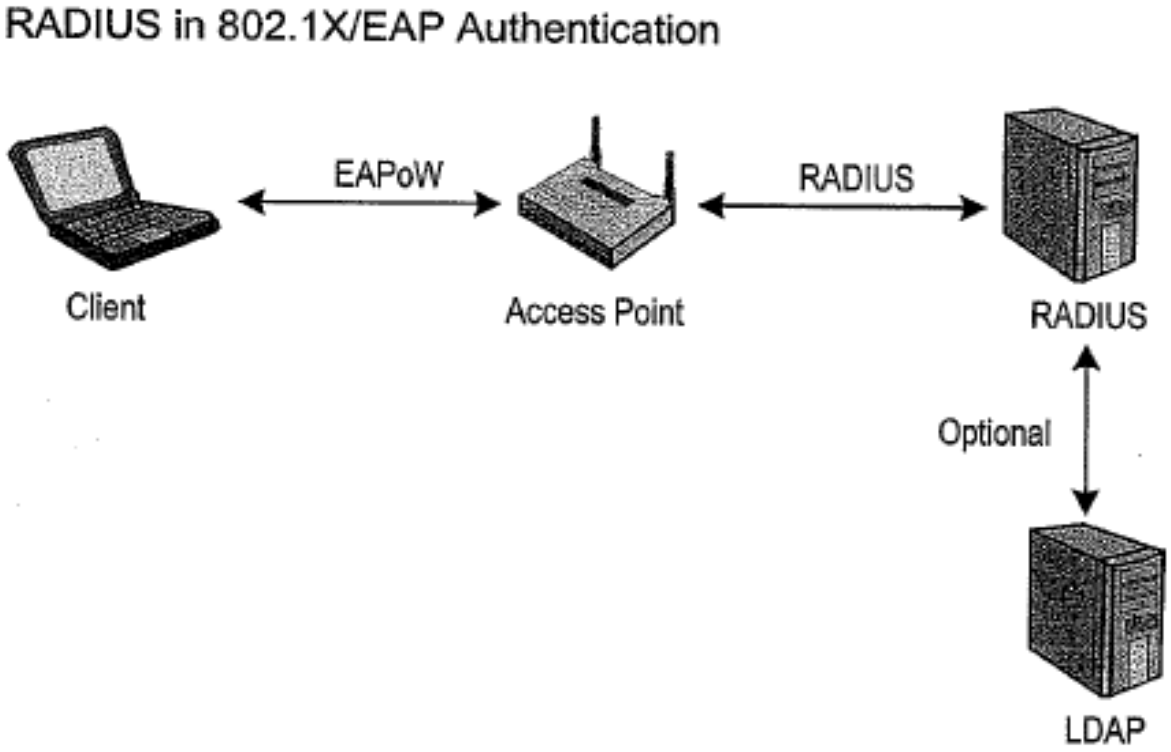
EAP-TTLS


802.11 Authentication & Association
802.1x / EAP Protocol Exchange
Select EAP-TTLS Authentication
802.1x / EAP-TLS Protocol Exchange & Client authenticates Server
Secure Tunnel Established
User's credentials exchanged using EAP-MD5, MS-CHAPv2, MS-CHAP, or PAP
EAP Success - User Authenticated - Key Material
EAP Success - Set WEP Keys
Encrypted data traffic allowed

RADIUS/AAA

- Remote Authentication Dial In User Service (RADIUS) is an AAA (authentication, authorization and accounting) protocol .
- AAA are used to manage credentials, provide profiles for what different roles can perform, and track resources.
- The three components to AAA are:
  - Authentication – allows an entity to provide credentials and asserts to identify.
  - Authorization – declines what functions the entity is permitted to perform.
  - Accounting – provides a way of logging and recording usage information.

Cont…


RADIUS in 802.1X/EAP Authentication
EAPoW
RADIUS
Client
Access Point
RADIUS
Optional
LDAP

Cont…

- Some common RADIUS features include:
  - Scalability
  - EAP support
  - Clustering and Failover Support
  - Accounting
  - Role Based Access Control
  - VLAN Tagging
  - Legacy Authentication Protocol Support
  - Mutual Authentication Support
  - Multiple Vendor Support
  - Software and Appliance Implementation

Authentication Design Considerations

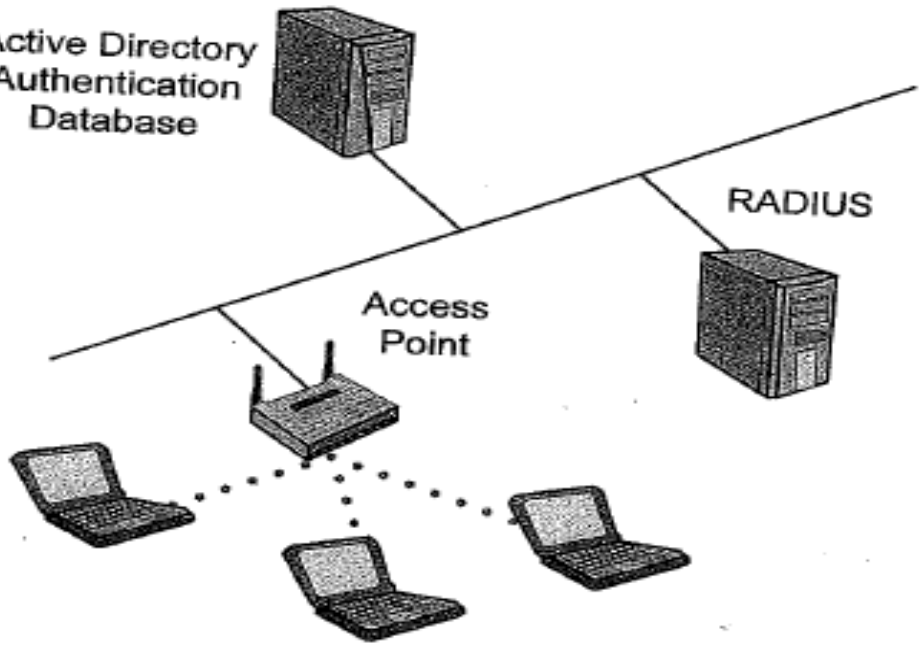
- Typical deployment Scenarios for RADIUS include:
  - Single site deployment
  - Distributed autonomous sites
  - Distributed Sites, Centralized Authentication & Security
  - Distributes Sites & Security, centralized Authentication
  - Combination Architectures.

Single Site Deployment

- This scenario is characterized as follows:
  - All WLAN users are located at a single site.
  - A central authentication database handles all user authentication.
  - One or more RADIUS servers manage WLAN and/or remote access use, authenticating users and setting up secure WLAN connections.

Cont…

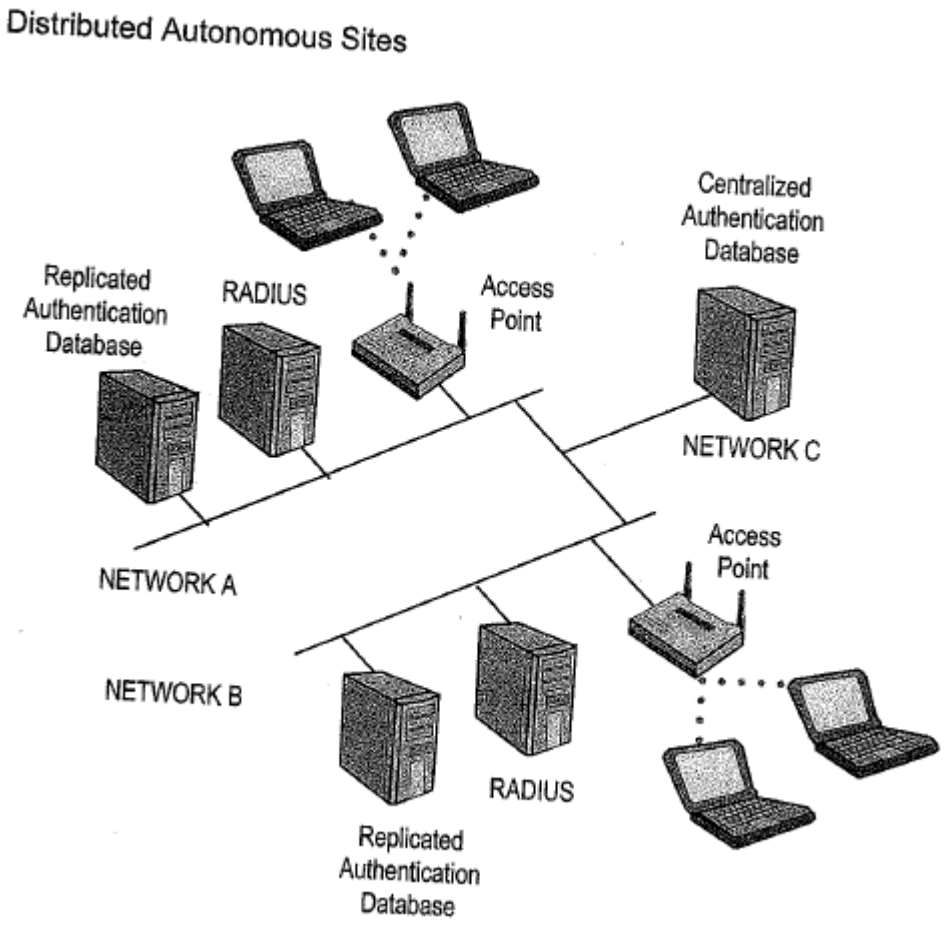
Single Site Deployment



Distributed Autonomous Sites

- This scenario is characterized as follows:
  - Distributed Autonomous Sites or networks.
  - The authentication database is replicated from the central site downstream to each autonomous site or network, so that all user authentication happens locally.
  - One or more RADIUS servers managing WLAN and/or remote access use are located at each autonomous site or network.

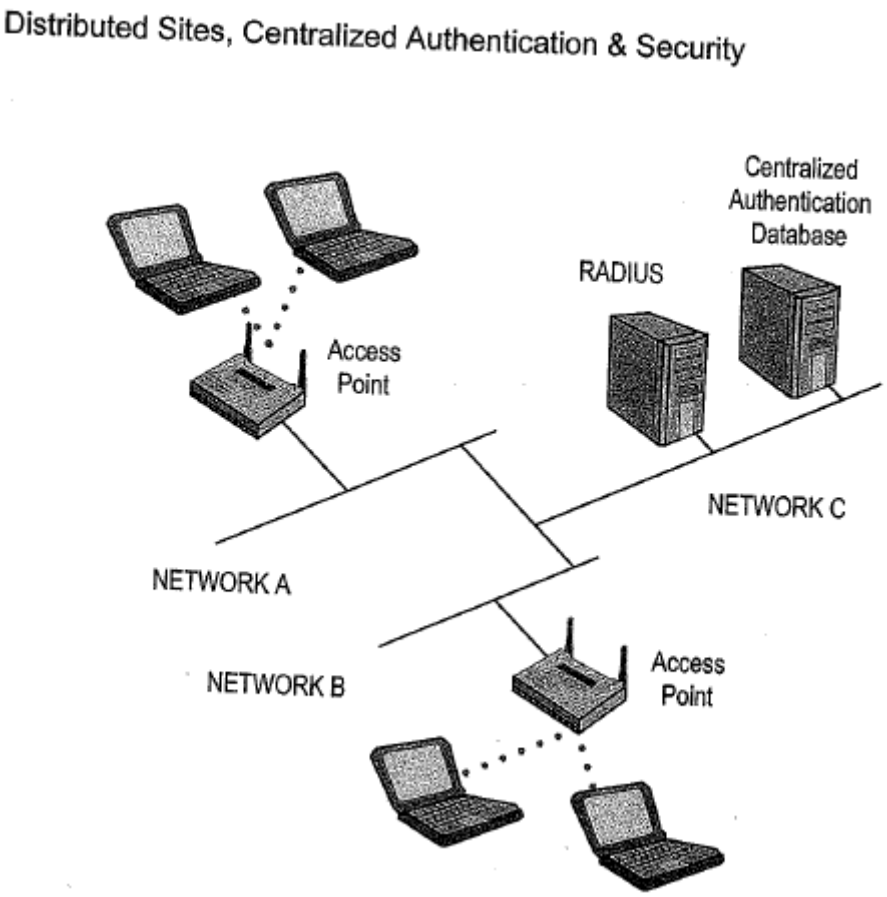
Cont…


Distributed Autonomous Sites
Centralized Authentication Database
Replicated Authentication Database
RADIUS
Access Point
NETWORK C
NETWORK A
Access Point
NETWORK B
RADIUS
Replicated Authentication Database

Distributed Sites, Centralized Authentication & Security

- This scenario is characterized as follows:
  - Distributed sites, networks, or clusters of access points.
  - WLAN access points at each site or on each network authenticate users against an authentication database located at a central site or operating hub.
  - One or more RADIUS servers at the central site manage all WLAN and/or remote access use.

Cont…

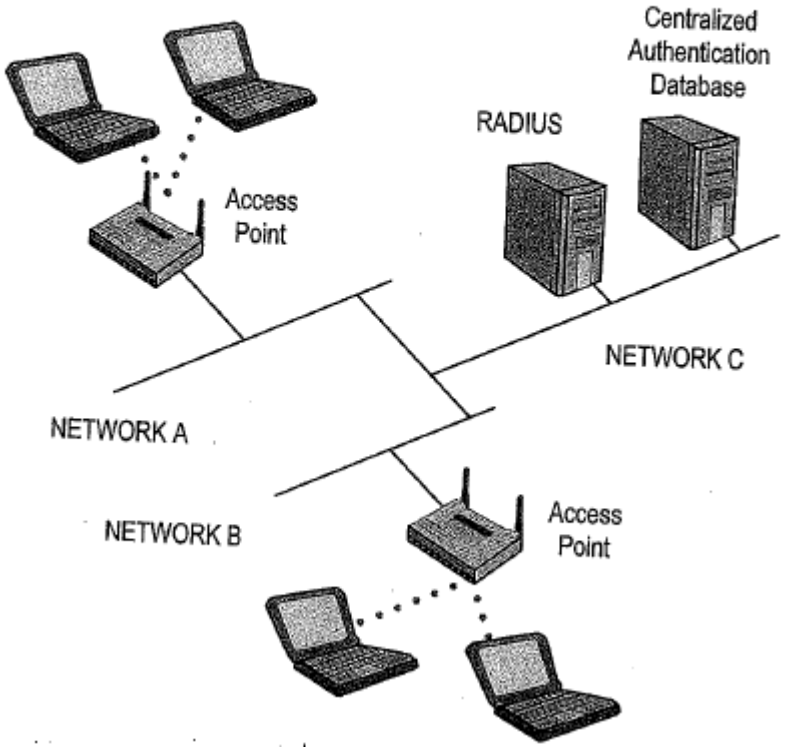

Distributed Sites, Centralized Authentication & Security
Centralized
Authentication
Database
RADIUS
Access
Point
NETWORK C
NETWORK A
NETWORK B
Access
Point

Distributes Sites & Security, centralized Authentication

- This scenario is characterized as follows:
  - Distributed sites, networks, or clusters of access points.
  - The authentication database is located at a central site or network hub.
  - One or more RADIUS servers managing WLAN and/or remote access use are located at each site, network ,or AP cluster.

Cont…

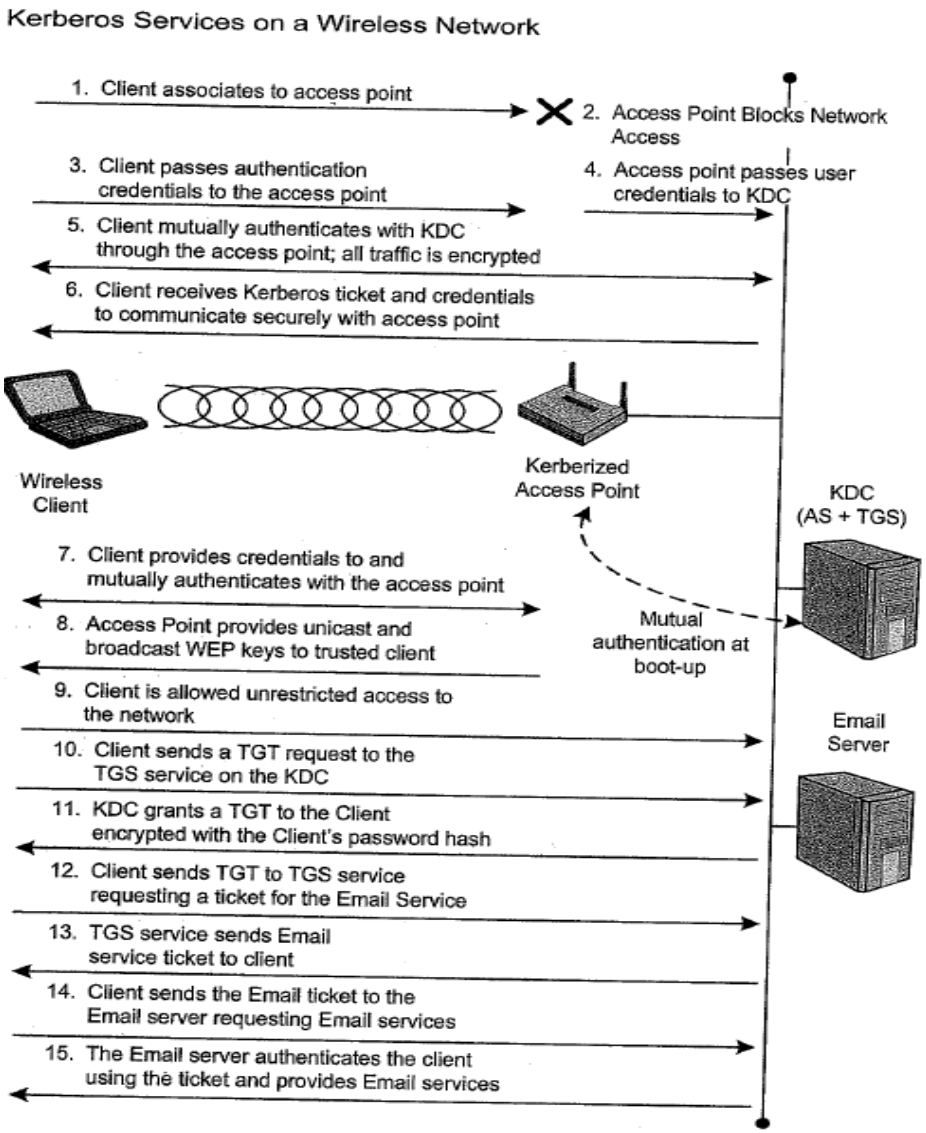
Distributed Sites, Centralized Authentication & Security



Kerberos

- Kerberos allows individuals communicating over a non-secure network to prove their identity to one another in a secure manner.
- It is also a suite of free software published by Massachusetts Institute of Technology (MIT) that implements this protocol.
- Its designers aimed primarily at a client-server model, and it provides mutual authentication — both the user and the server verify each other's identity.
- Kerberos protocol messages are protected against eavesdropping and replay attacks.

Cont…


Kerberos Services on a Wireless Network
1. Client associates to access point
2. Access Point Blocks Network Access
3. Client passes authentication credentials to the access point
4. Access point passes user credentials to KDC
5. Client mutually authenticates with KDC through the access point; all traffic is encrypted
6. Client receives Kerberos ticket and credentials to communicate securely with access point
Wireless Client
Kerberized Access Point
KDC (AS + TGS)
7. Client provides credentials to and mutually authenticates with the access point
8. Access Point provides unicast and broadcast WEP keys to trusted client
Mutual authentication at boot-up
9. Client is allowed unrestricted access to the network
Email Server
10. Client sends a TGT request to the TGS service on the KDC
11. KDC grants a TGT to the Client encrypted with the Client's password hash
12. Client sends TGT to TGS service requesting a ticket for the Email Service
13. TGS service sends Email service ticket to client
14. Client sends the Email ticket to the Email server requesting Email services
15. The Email server authenticates the client using the ticket and provides Email services

LDAP

- Lightweight Directory Access Protocol is a data retrieval protocol that information storehouses can implement that provides an inter-application exchange interface.
- LDAP binds together system information distributed across multiple computers with system services and client applications.
- LDAP can work in conjunction with RADIUS in order to authenticate users.
- LDAP is important in RADIUS implementations because RADIUS servers are commonly configured to query LDAP compliant or compatible databases for user authentication.
- LDAP acts as:
  - A Data Retrieval Protocol
  - An Application Service Protocol
  - An inter-application data exchange interface
  - A system service protocol.

Conclusion

- To help address the unauthorized access, 802.1X was developed to provide a standard mechanism for port-based authentication.
- Through the use of standard authentication messaging protocols provided by EAP, multi-vendor solutions are being created to support network authentication.
- Illustrated in detail the three types of authentication servers RADIUS, Kerberos and LDAP.

Source: white paper on 802.1X Authentication & EAP by Foundry Networks.