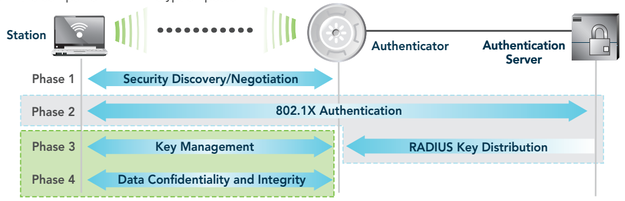
Wi-Fi™ REFERENCE SERIES

XIRRUS®

Wi-Fi AUTHENTICATION DEMYSTIFIED

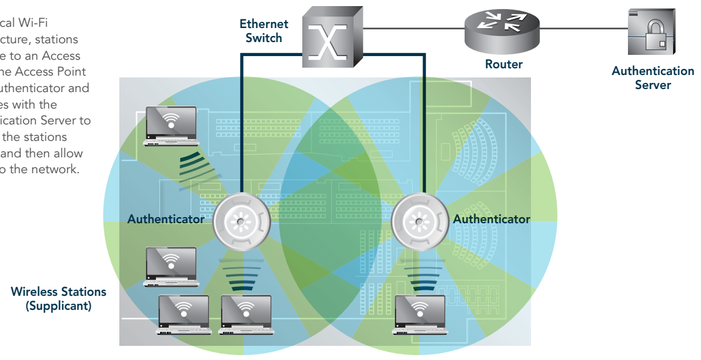
802.11n SECURITY

802.11i is the official security standard for 802.11 Wireless LANs as ratified by the IEEE in 2004. Its operation consists of 4 primary phases to establish secure communications. Phase 2 and portion of Phase 3 are addressed in this poster; Phase 4 and a portion of Phase 3 are addressed in the companion Wi-Fi Encryption poster.



TYPICAL Wi-Fi INFRASTRUCTURE

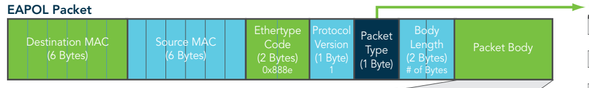
In a typical Wi-Fi infrastructure, stations associate to an Access Point. The Access Point is the Authenticator and interfaces with the Authentication Server to validate the stations identity and then allow access to the network.



EAPOL/EAP FRAME FORMAT

EAPOL (EAP Over LAN) is used by 802.1X to encapsulate the EAP protocol. The EAP protocol defines a number of methods for authentication.

EAPOL Packet



Value	Description
0	EAP Packet
1	EAPOL Start
2	EAPOL Logoff
3	EAPOL Key
4	EAPOL Alert

Value	Description
1	Request
2	Response
3	Success
4	Failure

EAP Packet

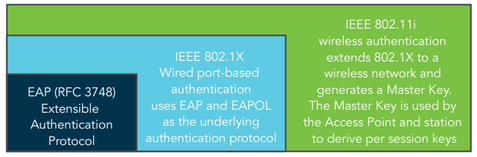
Value	Description	Value	Description
1	Identity	5	One Time Password
2	Notification	6	Generic Token Card
3	NAK	13	TLS
4	MD5 Challenge		

EAP TYPES

EAP Type	Description	Server Side Certificate	Client Side Certificate	User Credentials Used	User Database Access	Security Issues
EAP-PEAP	Protected EAP (widely used)	Required	Optional	Windows XP, 2000, CE, Username/Passwords and other 3rd party Supplicants	Windows Domains, Active Directory	
EAP-TLS	EAP with Transport Layer Security	Required	Required	Certificate	Windows Domains, Active Directory, Novel NDS OTP	User Identity Exposed
EAP-TTLS	EAP with Tunneled Transport Layer Security	Required	None	Password	Windows Domains, Active Directory	
EAP-PEAP-GTC	Protected EAP with Generic Token Card	Required	None	Windows, Novell NDS, One Time Password Token		
EAP-SIM	EAP – Subscriber Identity Module (SIM). Uses SIM card found in GSM mobile phone handsets	Required	None	Subscriber Identity Module (SIM Card)		
LEAP	Lightweight EAP. Not recommended due to dictionary attacks	None	None	Password	Windows Domains, Active Directory	Dictionary Attack User Identity Exposed
Fast EAP	Cisco EAP based on PEAP	None	None	Password	Windows Domains, Active Directory	

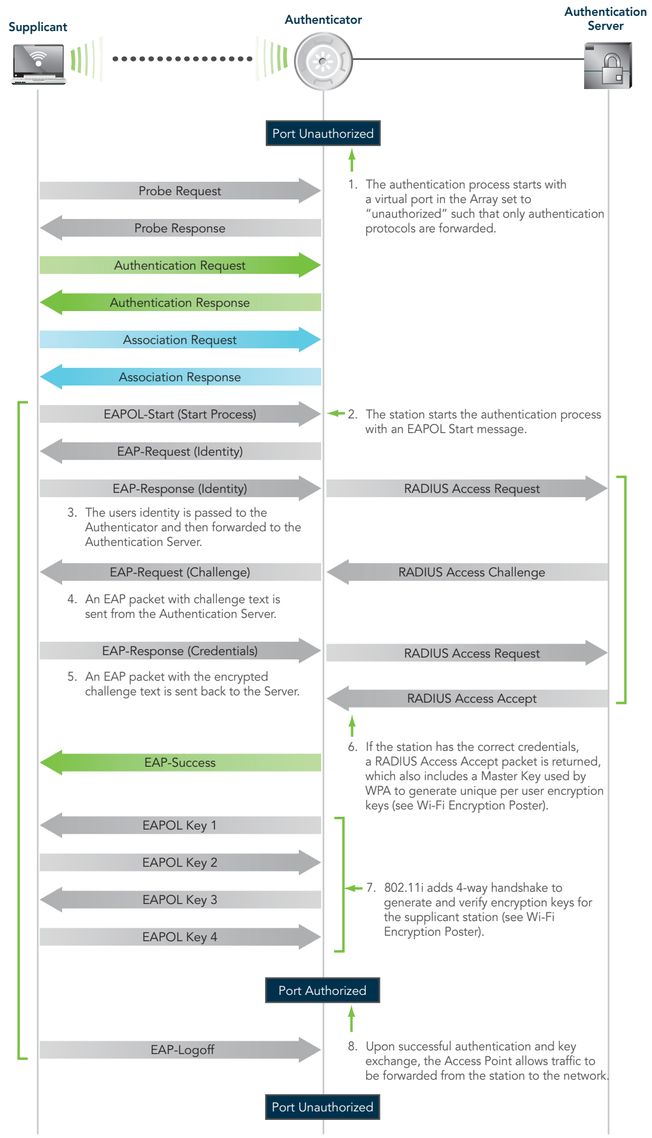
WIRELESS AUTHENTICATION FRAMEWORK

Wi-Fi Authentication (802.11i) is built on top of 802.1X and EAP.



802.11i PACKET EXCHANGE

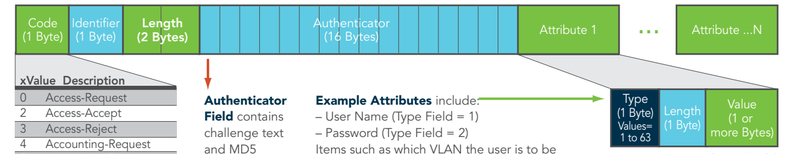
802.11i Packet Exchange describes the wireless authentication process, and begins with a supplicant (the wireless station) associating to the access point and initiating an 802.1X exchange.



1. The authentication process starts with a virtual port in the Array set to "unauthorized" such that only authentication protocols are forwarded.
2. The station starts the authentication process with an EAPOL Start message.
3. The users identity is passed to the Authenticator and then forwarded to the Authentication Server.
4. An EAP packet with challenge text is sent from the Authentication Server.
5. An EAP packet with the encrypted challenge text is sent back to the Server.
6. If the station has the correct credentials, a RADIUS Access Accept packet is returned, which also includes a Master Key used by WPA to generate unique per user encryption keys (see Wi-Fi Encryption Poster).
7. 802.11i adds 4-way handshake to generate and verify encryption keys for the supplicant station (see Wi-Fi Encryption Poster).
8. Upon successful authentication and key exchange, the Access Point allows traffic to be forwarded from the station to the network.

RADIUS

RADIUS (RFC 2138) defines the backend authentication process between the Authenticator and Authentication Server. RADIUS Attributes carry specific authentication, authorization, information and configuration detail for the Access request and response types.



xValue	Description
0	Access-Request
2	Access-Accept
3	Access-Reject
4	Accounting-Request
5	Accounting-Response
11	Access-Challenge
12	Status-Server (experimental)
13	Status-Client (experimental)
255	Reserved

Authenticator Field contains challenge text and MD5 hashed responses (passwords)

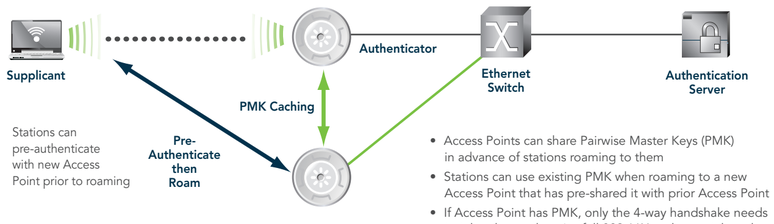
Example Attributes include:
– User Name (Type Field = 1)
– Password (Type Field = 2)
Items such as which VLAN the user is to be assigned to or what wireless user group policies to use can be defined by the use of Vendor Specific Attributes (VSAs) (Type Field = 26).

WEB-BASED AUTHENTICATION

Web-Based Authentication eliminates need to configure client software but requires manual entry of username/password. It is not used to configure an encrypted wireless link.

1. A user associates to an open Wi-Fi network
2. User's web session is captured and redirected to a landing page in the Access Point
3. The user is prompted for a username and password
4. The Access Point uses these credentials to authenticate the user with the Authentication Server
5. Access is granted and the user's original URL is reloaded

802.11i FAST ROAMING



Stations can pre-authenticate with new Access Point prior to roaming

- Access Points can share Pairwise Master Keys (PMK) in advance of stations roaming to them
- Stations can use existing PMK when roaming to a new Access Point that has pre-shared it with prior Access Point
- If Access Point has PMK, only the 4-way handshake needs to take place, otherwise full 802.11X exchange takes place

GLOSSARY

802.1X—An IEEE standard for port-based network access control. It provides authentication services for devices attached to a wired network port.

802.11i—An 802.11i is a 2004 IEEE standard that specifies TKIP and AES encryption, and 802.1X authentication for 802.11 networks. This supersedes the previous WEP (Wired Equivalent Privacy) specification from the original 802.11 specification which has since been found to be easily compromised.

Authenticator—The end of the link initiating EAP authentication. Normally, this is the Access Point in an 802.11 environment.

Authentication Server—An entity that provides an authentication service to an authenticator. When used, this server typically executes EAP methods for the authenticator. In an 802.11 environment this is normally a RADIUS server.

Certificate—An element used to authenticate the identity and source of a message. Public-private key cryptography is used to create and digitally sign the certificate.

EAP—Extensible Authentication Protocol is defined by RFC 3748 and is a framework for authentication. EAP itself does not define the underlying authentication protocol to be used.

EAPOL—EAP Over LAN is the 802.1X encapsulation of EAP messages.

Pairwise Master Key—A unique per-user encryption key that is derived from the station's 802.1X exchange from which transient keys are created and used to encrypt data between the station and the Access Point.

Remote Authentication Dial In User Service (RADIUS)—An Authentication, Authorization and Accounting (AAA) protocol for user access to a wired or wireless network.

Supplicant—The end of the link that responds to the authenticator. In an 802.11 environment this is normally the wireless station.

WPA—Wi-Fi Protected Access (WPA/WPA2). A Wi-Fi Alliance specification implementing TKIP and AES encryption plus 802.1X authentication for 802.11 networks. This supersedes the previous WEP (Wired Equivalent Privacy) specification from the original 802.11 specification which has since been found to be easily compromised.

+805.262.1600 • 800.947.7871 • posters@xirrus.com • www.xirrus.com