

Demystifying Wireless Network Access and 802.1X Security

The openness of wireless networks brings uncertainty to network managers and users. The network manager wants to limit access to his network to only authorized users and a user needs assurance he is accessing the right network. This paper provides insight into the typical wireless LAN client login process and 802.1X and EAP authentication processes.

[Table of contents](#)

| | |
|---|-----------|
| Network access and security overview . . | 2 |
| Typical 802.1X authentication process . . | 3 |
| EAP versions | 4 |
| Typical client login process | 4 |
| Example 1: EAP TLS authentication. | 5 |
| Example 2: LEAP authentication | 8 |
| Example 3: PEAP-MS-CHAP-V2 authentication. | 9 |
| Summary and references | 11 |

Demystifying Wireless Network Access and 802.1X Security

Network managers and network users are concerned about network access and security. A network manager wants assurance that the client requesting access to his network is really who they say they are – an authorized user and not an imposter. Similarly, a network user wants assurance that when he connects his wireless notebook PC to his network, he is really connecting to his network – and not to a counterfeit network thrown together by a hacker to intercept user information. It is essentially an issue of trust – for both network managers and users.

Some of the first security and privacy schemes developed to provide this trust have proven vulnerable to hacker attacks – 802.11's Wired Equivalent Privacy (WEP), for example. Today's network manager is looking to 802.1X to provide a secure environment he can trust. To date, 802.1X is living up to this promise.

The IEEE published the 802.1X standard, "Port Based Network Access Control," on December 13, 2004. It is available at <http://standards.ieee.org/getieee802/802.1.html>. The 802.1X standard provides a means of authenticating and authorizing devices attempting to attach to a local area network, and prevents access to the LAN in cases where the authentication and authorization process fails.

Managers of wireless LANs were among the first to implement 802.1X. WLANs are not physically secured behind walls and locked doors like a wired network, making them more susceptible to attack. 802.1X is now seeing more use in wired networks, too, as an added security measure.

IEEE 802.1X evolved from Point-to-Point Protocol (PPP) and Extensible Authentication Protocol (EAP). PPP is most commonly used for dial-up Internet access. It includes an authentication mechanism consisting of a user name and password. EAP was developed to provide a more robust security mechanism. EAP resides within PPP's authentication protocol and provides a generalized framework for several different authentication methods. EAP is defined in IETF's RFC 3748, available at <http://www.ietf.org/rfc>. IEEE 802.1X is a standard for passing EAP over a wired or wireless LAN. 802.1X does not use PPP; rather EAP messages are packaged in Ethernet frames. This encapsulation of EAP packets is known as "EAP over LANs," or EAPOL.

IEEE 802.1X defines three necessary roles to complete an authentication exchange. The authenticator is the network device (i.e. access point, switch) that wishes to enforce authentication before allowing access. The supplicant is the network device (i.e. client PC, PDA) requesting access. The authentication server, typically a RADIUS server, performs the authentication function necessary to check the credentials of the supplicant on behalf of the Authenticator and indicates whether the supplicant is authorized to access the Authenticator's services. Although it is possible to combine the roles of authenticator and authentication server in a single device, the usual implementation involves independent devices. This is particularly helpful when engineering a wireless network in that most of the work is being performed by the supplicant (a wireless notebook PC) and the authentication server – the authenticator (the access point) can be smaller with less processing power and memory.

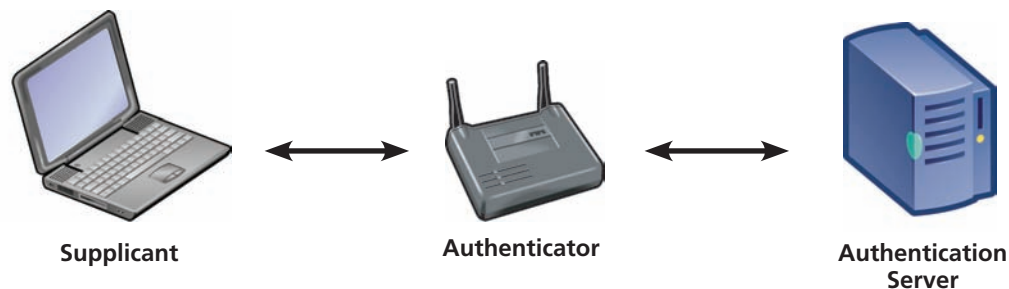


























Figure 1: 802.1X roles

Following is a typical, successful 802.1X authentication process. The process is initiated as soon as the Supplicant detects an active link (e.g., notebook PC has associated with the access point).

| From | To | EAP Packet content | Purpose |
|---|---|---------------------------------|--|
|  |  | EAP Start | Request to start the EAP authentication process |
|  |  | EAP - Request/Identity | Requesting authentication before allowing access |
|  |  | EAP - Response/Identity | Responding to request with identity information |
|  |  | EAP - Response/Identity | Passes request to Authentication Server |
|  |  | Challenge | Sends request for authentication information. There are several different EAP versions so the challenge can vary (i.e. username/password, user certificate.) |
|  |  | Challenge | Encapsulates challenge with EAPOL and sends to supplicant. |
|  |  | Challenge response | Sends challenge response. |
|  |  | Challenge response | Decodes response and sends to Server. |
|  |  | Success message and session key | Success message and session key sent only if the Supplicant sent the correct response and the Server can validate it's identity. |
|  |  | Success message | Supplicant successfully authenticated. |
|  |  | Key exchange | Create encryption keys using the session key. |
|  |  | Key Exchange Response | Encryption keys set. |

There are many versions of EAP. They generally differ in the complexity and security of the challenge processes. Some of the challenge processes authenticate only the client while others facilitate mutual authentication of both client and network. Some utilize encryption of challenge requests and responses. The most common EAP types are those built into switches, routers and operating systems as these are usually easiest to implement. The following table lists some of the more common EAP types used with 802.1X.

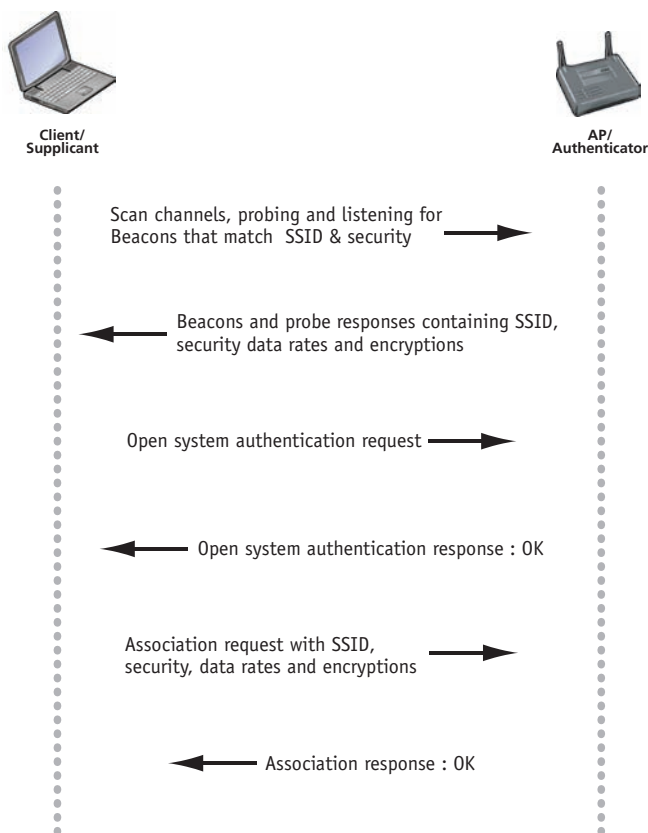
| EAP Type | Name | LAN Type |
|---------------------|--|-------------------|
| EAP-TLS | EAP Transport Layer Security | Wireless Wired |
| EAP-GTC | EAP Generic Token Card | Wired |
| EAP-MD5 | EAP Message Digest 4 | Wired |
| EAP-MS-CHAP-V2 | EAP Microsoft Challenge Handshake Authentication Protocol version 2 | Wired |
| EAP-FAST | EAP Flexible Authentication via Secure Tunneling | Wireless |
| LEAP | Lightweight EAP | Wireless |
| PEAP-GTC | Protected EAP Generic Token Card | Wireless Wired |
| PEAP-MD5 | Protected EAP Message Digest 5 | Wireless Wired |
| PEAP-MS-CHAP-V2 | Protected EAP Microsoft Challenge Handshake Authentication Protocol version 2 | Wireless Wired |
| PEAP-TLS | Protected EAP Transport Layer Security | Wireless Wired |
| TTLS-PAP | Tunneled Transport Layer Security Password Authentication Protocol | Wireless Wired |
| TTLS-CHAP | Tunneled Transport Layer Security Challenge Handshake Authentication Protocol | Wireless Wired |
| TTLS-MS-CHAP | Tunneled Transport Layer Security Microsoft Challenge Handshake Authentication Protocol | Wireless Wired |
| TTLS-MS-CHAP-V2 | Tunneled Transport Layer Security Microsoft Challenge Handshake Authentication Protocol version 2 | Wireless Wired |
| TTLS-EAP-MD5 | Tunneled Transport Layer Security Message Digest 5 | Wireless Wired |
| TTLS-EAP-MS-CHAP-V2 | Tunneled Transport Layer Security Message Digest 5 Microsoft Challenge Handshake Authentication Protocol version 2 | Wireless Wired |
| TTLS-EAP-TLS | Tunneled Transport Layer Security | Wireless Wired |

Following are examples of the authentication processes for several of the most commonly employed EAP types: EAP-TLS, LEAP and PEAP-MSCHAP-V2. In the first example, we will add the wireless LAN association process and the IP address resolution process since these processes, along with the authentication process, are what typically constitute the client login process.

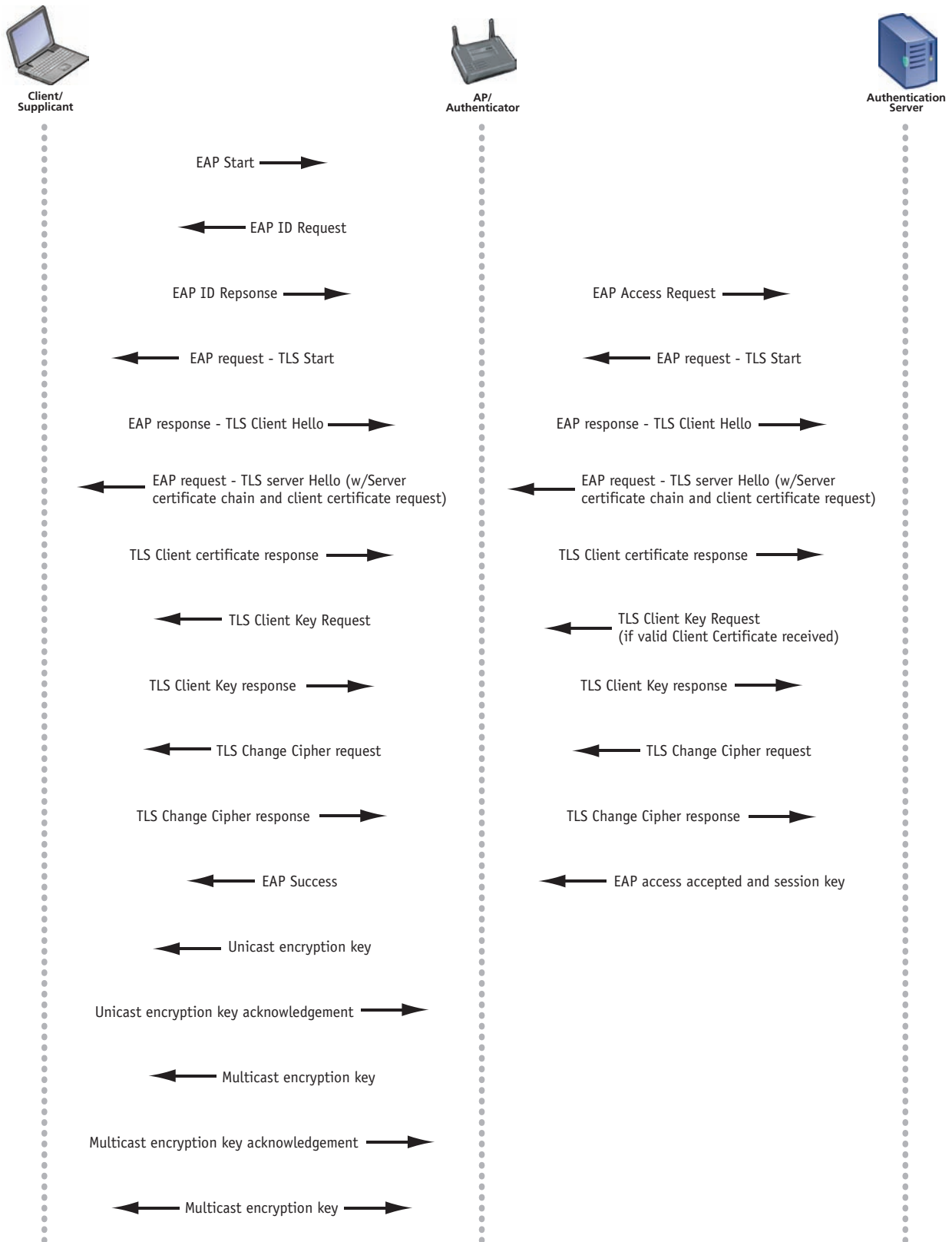


Figure 2: typical WLAN client login process

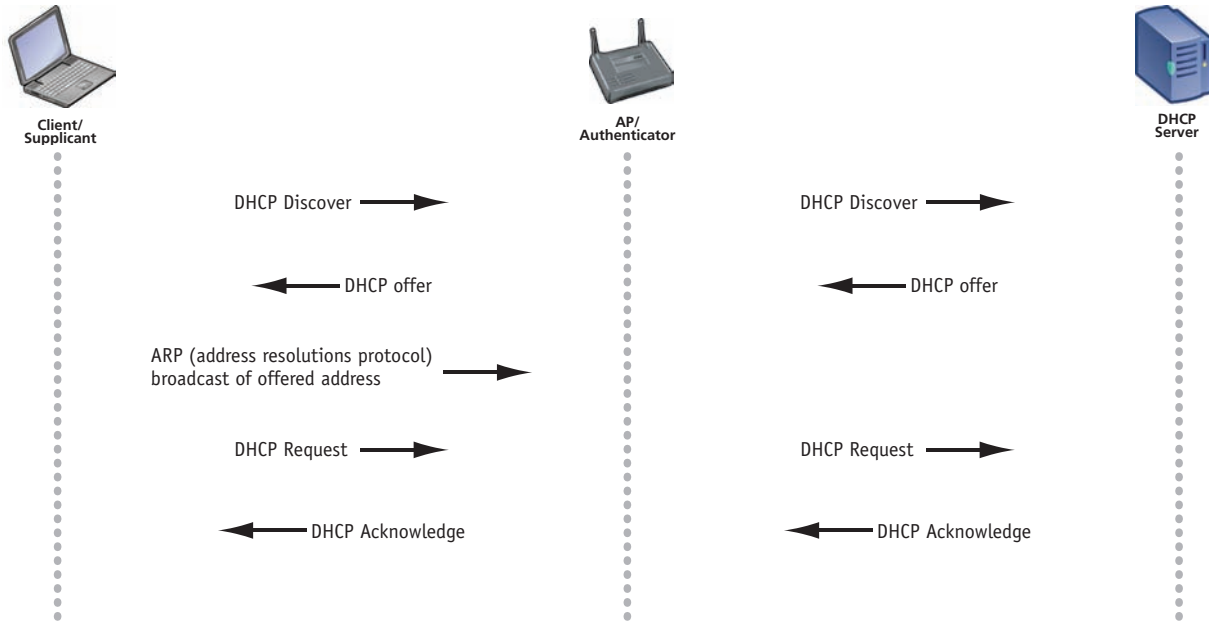
Example 1: WLAN login process with EAP TLS authentication



802.11 Association process



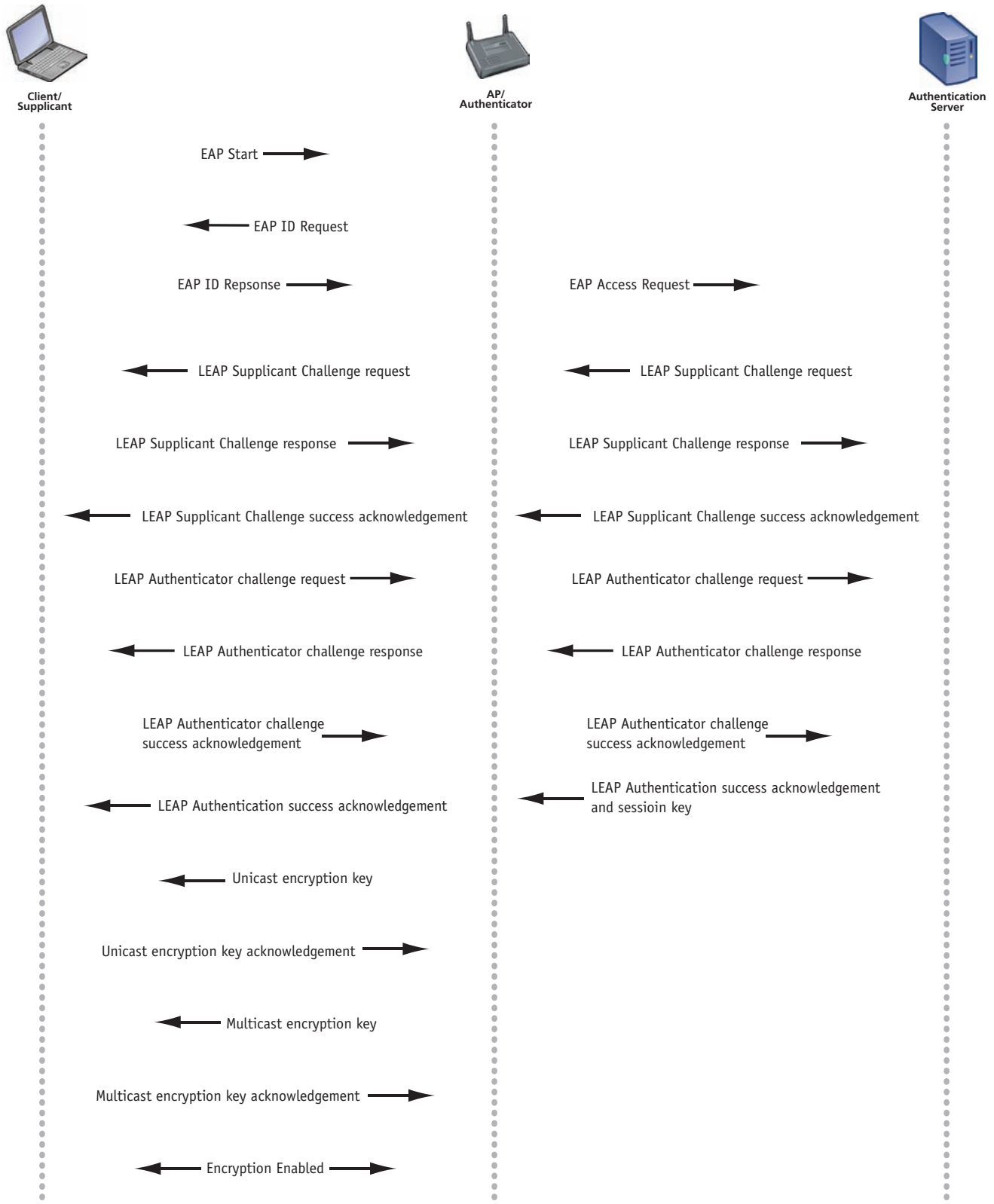
802.1X EAP-TLS Authentication process



DHCP IP address resolution process

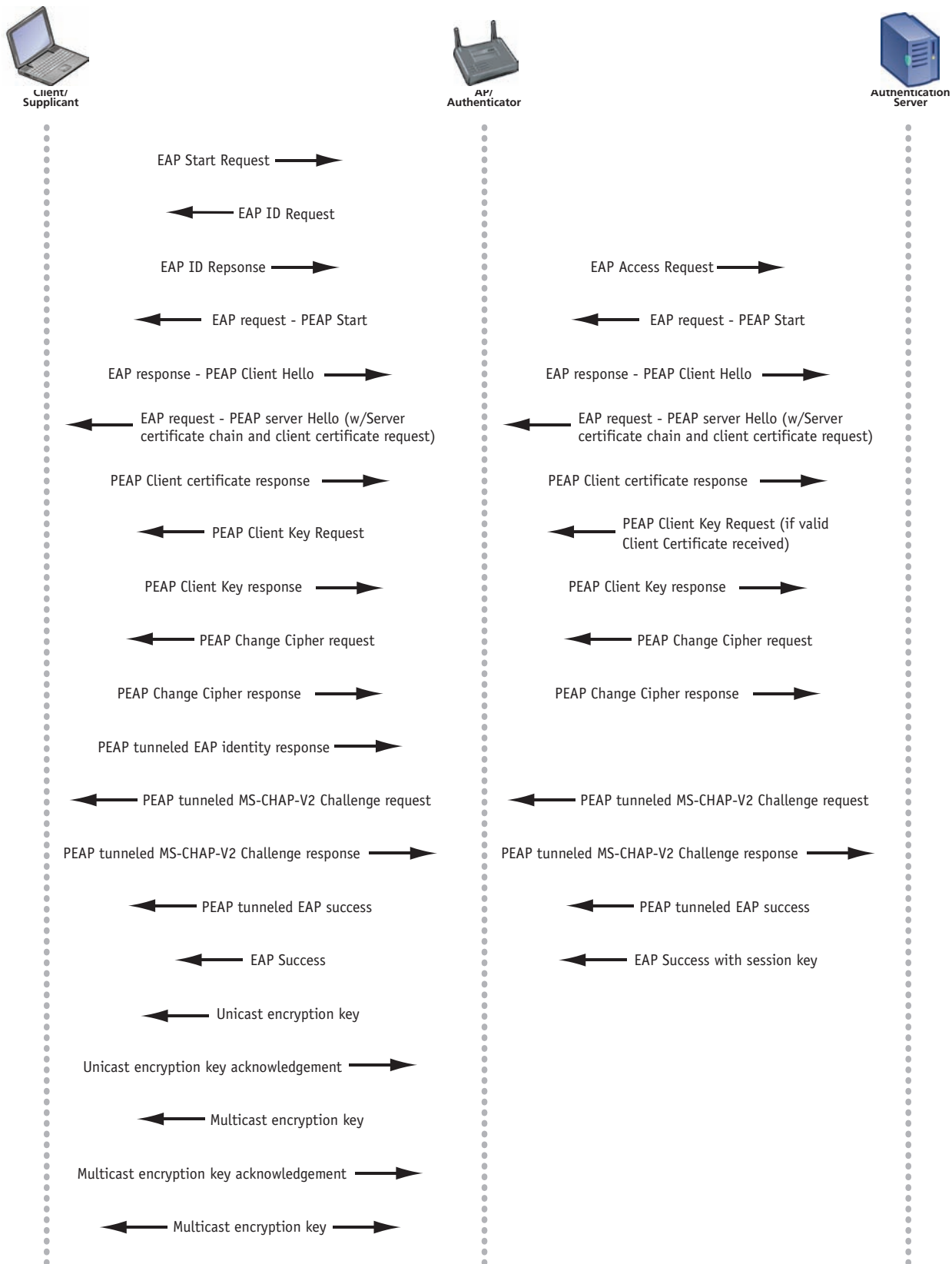
Example 2: 802.1X LEAP authentication

In this example, we are documenting only the LEAP authentication process. The wireless LAN association and DHCP processes are unchanged.



Example 3: 802.1X PEAP-MS-CHAP-V2 authentication process

In this example, we are documenting only the PEAP-MS-CHAP-V2 authentication process. The wireless LAN association and DHCP processes are unchanged.



Summary

An understanding of the association, authentication and IP address resolution processes can assist in troubleshooting client login problems. Network analysis tools are available that can monitor and log the entire client-to-network login process. If a valid wireless notebook PC user is unable to access the network, connect a network analyzer to your network and observe the entire login process. You will be able to isolate where the process fails. Once you isolate the problem through observation of these processes, you will know what's broken and what you need to fix or repair the process.

Authentication, the process of proving identity, is an essential component of network security. By implementing IEEE 802.1X authentication, network managers have an effective means of controlling access to their networks. There is a choice of EAP types; some developed for both wireless and wired LANs, others for just one category. Do a bit of research before selecting a type, as there are advantages and disadvantages of each. An understanding of the authentication and login-associated processes will assist you in troubleshooting user access problems. And remain vigilant to emerging security threats – it's the best way to establish trust in your network.

References

- IEEE Std 802.1X-2004, IEEE Standard for Local and metropolitan area networks, Port-Based Network Access Control.
- IETF RFC 3748, Extensible Authentication Protocol (EAP), Blunk, L., Vollbrecht, J., Aboba, B., Carlson, J., Levkowetz, H., June 2004
- Geier, Jim. "802.1X Offers Authentication and Key Management." Wi-Fi Planet 7 May 2002.
- Snyder, Joel. "What is 802.1X?" Network World Fusion 6 May 2002
- "802.1X Port Access Control for WLANs." Wi-Fi Planet.com 5 September 2003
- "Deploying 802.1X for WLANs: EAP Types." Wi-Fi Planet.com 10 September 2003

NETWORK SUPERVISION

Fluke Networks
P.O. Box 777, Everett, WA USA 98206-0777

Fluke Networks operates in more than 50 countries worldwide. To find your local office contact details, go to www.flukenetworks.com/contact.

©2006 Fluke Corporation. All rights reserved.
Printed in U.S.A. 04/2006 2647086 A-US-N Rev A