802.11b Wireless LAN Authentication, Encryption, and Security

Young Kim
ELEN 6951

1. Abstract

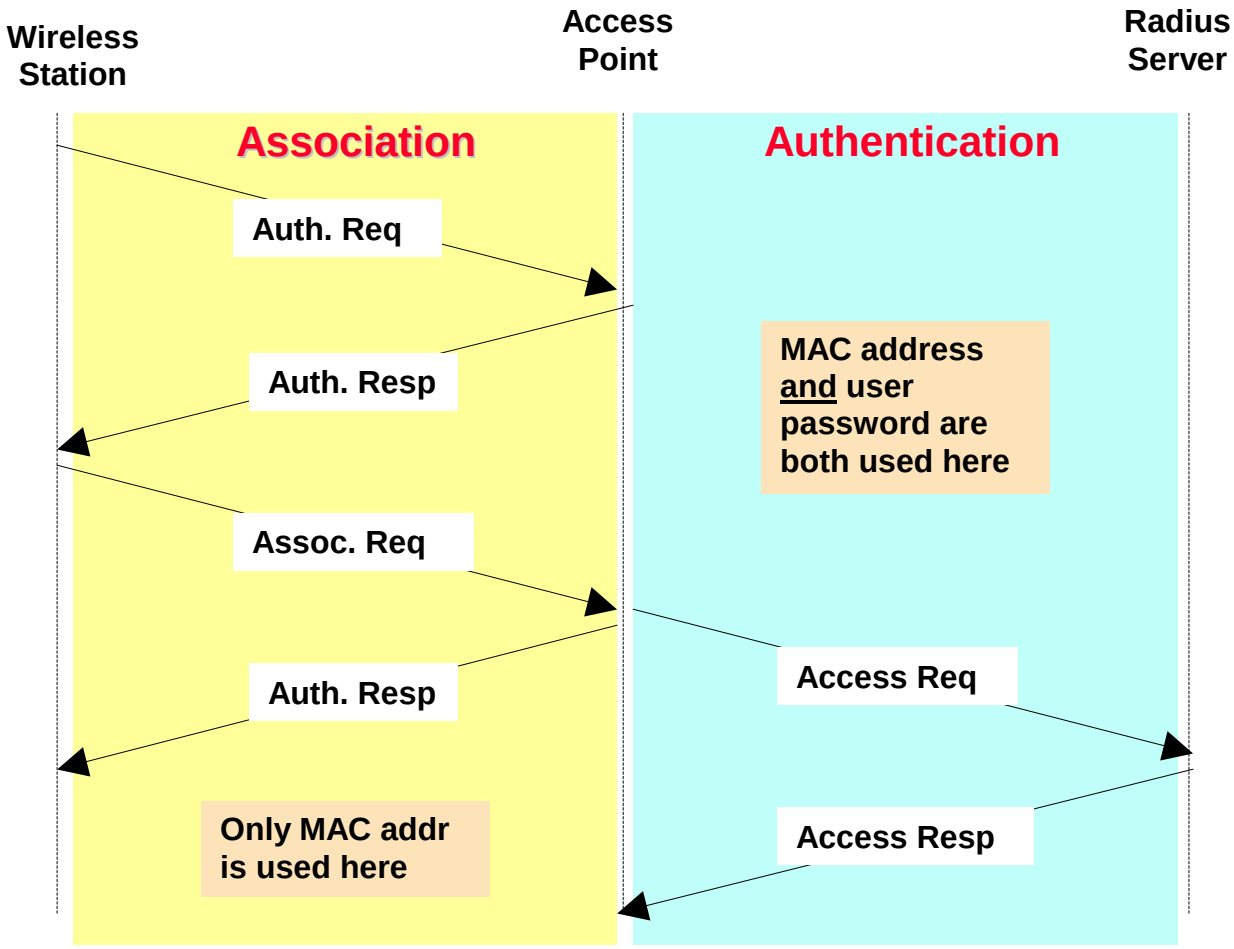
With the rapid growth of wireless local area network, security has been the number one concern in this arena of technology. Numerous of work is being done is this area to address this issue. This paper will provide technical details about 802.11b wireless authentication, encryption, and security mechanisms; mainly 802.1x standard and how when encryption used together with authentication can make wireless network less vulnerable.

2. Background

The IEEE 802.11 Wireless LAN is a standard that uses the carrier sense multiple access (CSMA), medium access control (MAC) protocol with collision avoidance (CA). This standard allows for both direct sequence (DS), and frequency-hopping (FH) spread spectrum transmissions at the physical layer. The maximum data rate initially offered by this standard was 2 megabits per second. A higher-speed version, with a physical layer definition under the IEEE 802.11b specification, allows a data rate of up to 11 megabits per second using DS spread spectrum transmission. The IEEE standards committee has also defined physical layer criteria under the IEEE 802.11a specification. This is based on orthogonal frequency-division multiplexing (OFDM) that will permit data transfer rates up to 54 megabits per second.

3. Security Mechanisms Overview

Service Set Identifiers (SSIDs) is a common network name that must be used by the mobile to gain access to Access Point (AP) which is attached to the network. Authentication is accomplished using SSID by the following way: Station will send out a probe frame (active scanning) with desired Service Set ID (SSID). AP will send back a probe response frame and finally STA will accept the SSID, Timing Sync Func (TSF), timer value, and PHY setup values from the AP frame. This however is a low security because the SSID may be sent by the AP in its broadcasted beacon frames. Therefore, IEEE 802.11 defines authentication and encryption services based on the Wired Equivalent Privacy (WEP) algorithm. WEP with 40-bit encryption key is required WiFi certification which is sanctioned by Wireless Ethernet Compatibility Alliance (WECA). Another method of authentication can be done with equipment's MAC address look-up table in the AP. An access control list is kept in each AP and centralized database records of users in RADIUS server (RFC2138). More information about RADIUS server will be discussed in the subsequent section. (RFC2138). Authentication is unique to the MAC address of the radio card. MAC address based Authentication is shown below:



However, MAC address based authentication is low security because the equipment can be stolen.

Despite the above security mechanisms mentions, the following security issues exist with 802.11:

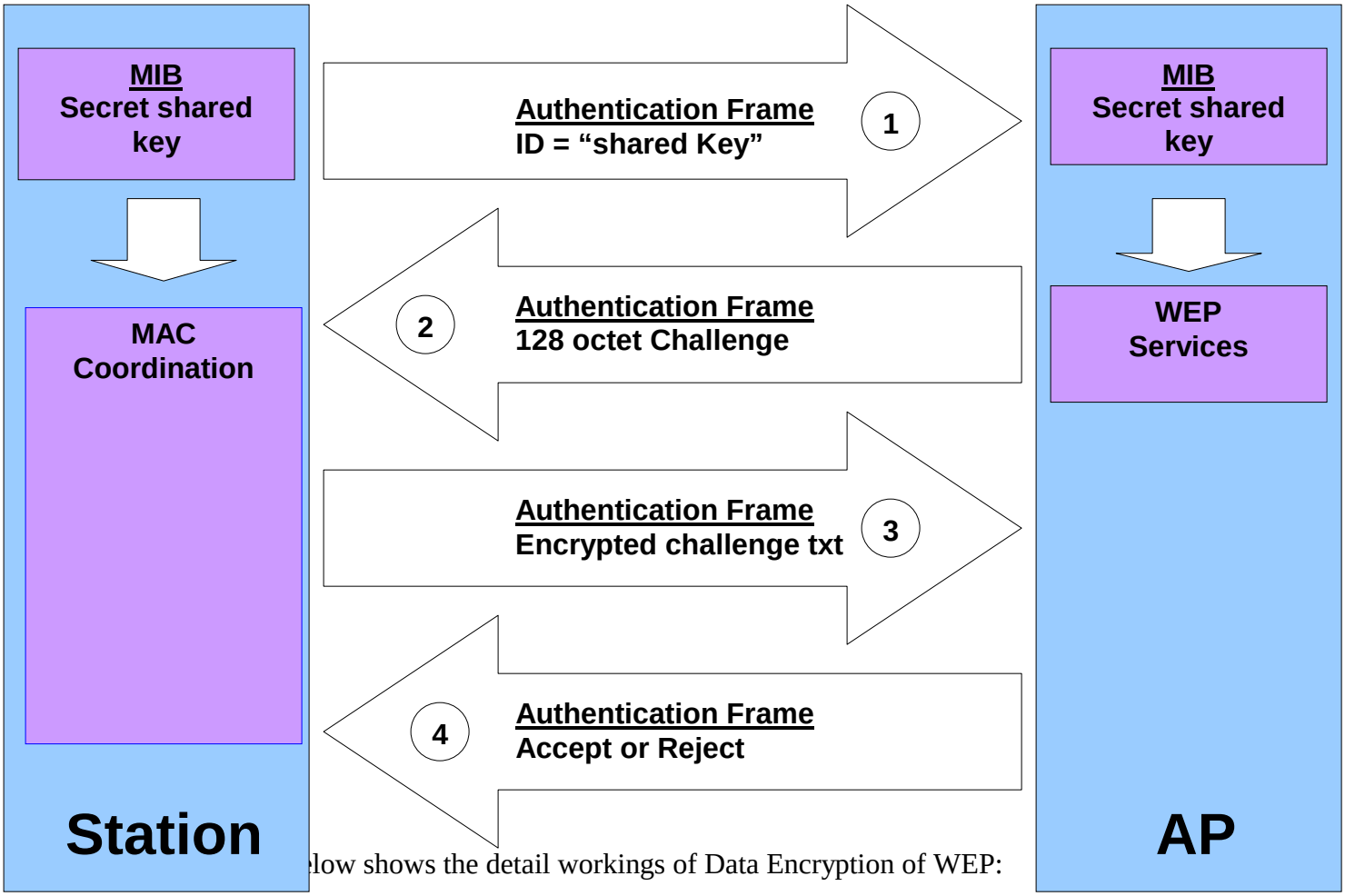
- No per-packet authentication
- Vulnerability to disassociation attacks
- No user identification and authentication
- No central authentication, authorization, and accounting support
- RC4 stream cipher is vulnerable to known plaintext attacks
- Some implementations derive WEP keys from passwords

- No support for extended authentication; for example: token cards; certificates/smart-cards; one-time passwords; biometrics; etc.
- There are key management issues; for example, re-keying global keys, and no dynamic, per-STA unicast session, key management

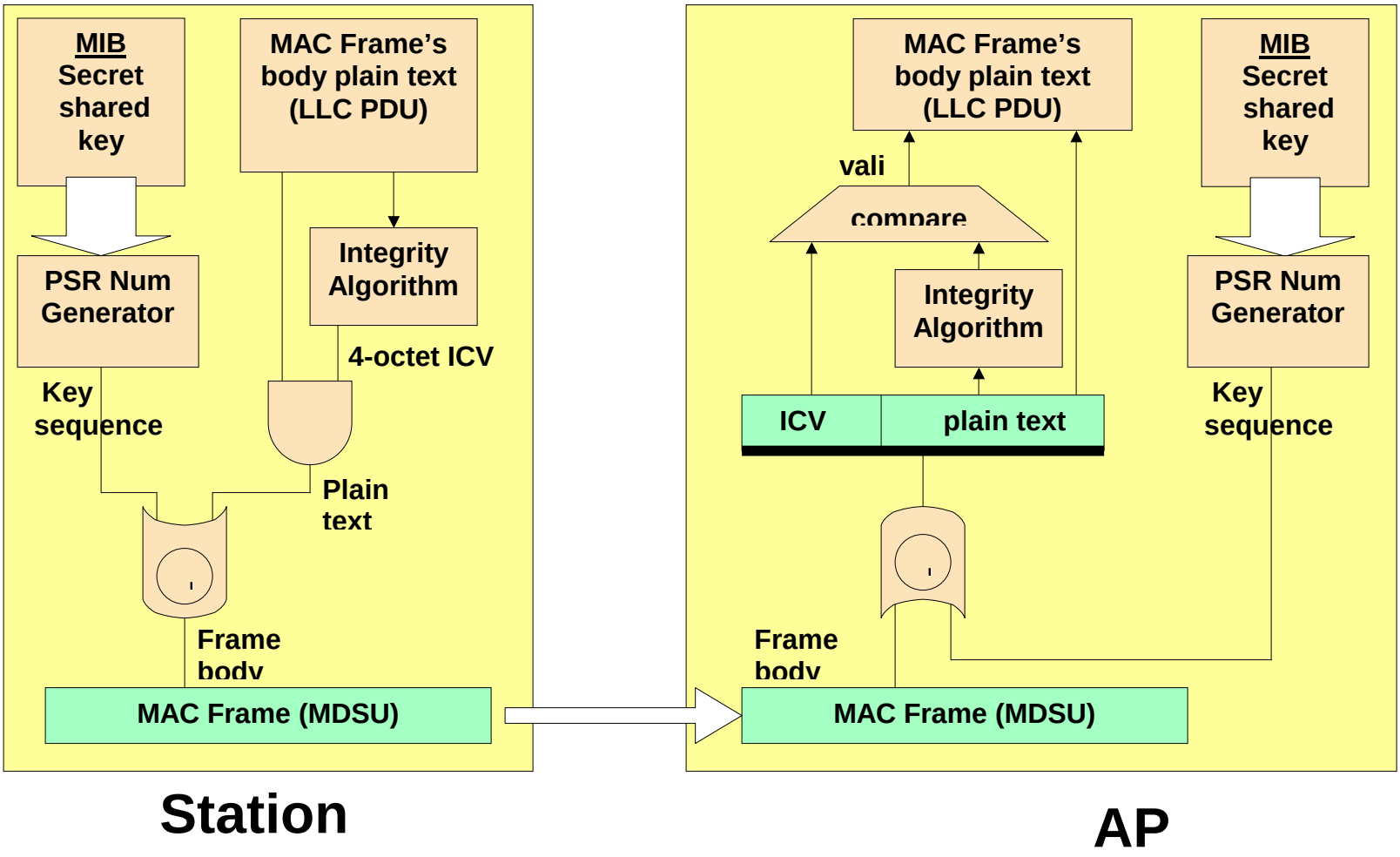
3. WEP Overview

WEP is a symmetric (encrypt and decrypt) data encryption algorithm. In shared in WEP algorithm user must have a shared WEP key that is same for both AP and STAs. Authentication uses the same WEP key in a CHAP exchange, where AP sends a challenge text packet and STA encrypts with the WEP key and sends to AP. So as you can see this is just a one-way authentication only and there is a danger that rouge AP can discover the key.

Below is a figure of shared key authentication using WEP:



elow shows the detail workings of Data Encryption of WEP:



WEP is an extension to the 802.1X protocol, which will be discussed in the next section, that provides a means for encryption of wireless communications. Encryption is provided through the use of WEP Keys. These keys may be manually configured on the end-station and the access point. In this case, the end-station is configured with one or two 40-bit WEP Keys to be used for authentication and encryption. If two keys are defined there is a unicast key associated with this particular end-station and a multicast key that will be used globally. If only one key is defined, then that key is the multicast key. These keys must match the same key(s) as is configured on the access point. Manual configuration presents a problem though, because both the access point and the end station know the WEP key. The WEP key will seldom change because it requires manual configuration at both the end station and the access point.

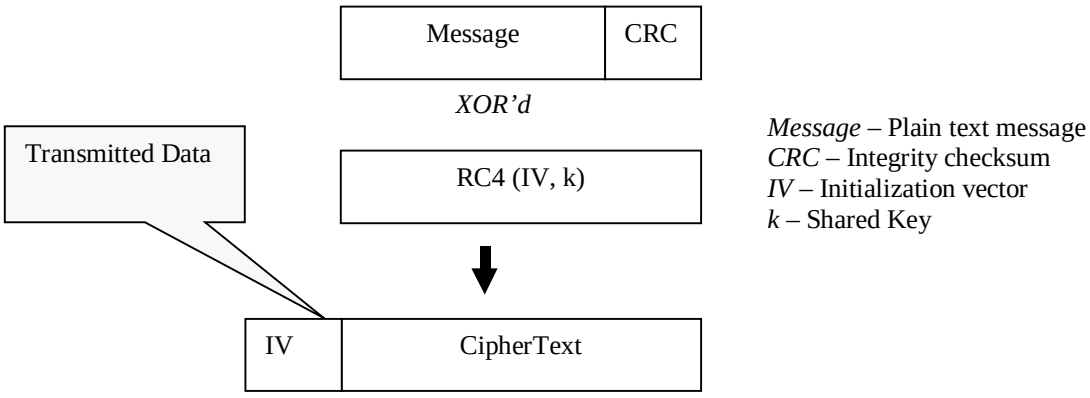


Figure: Encrypted WEP frame.

To illustrate the problem of using a WEP key as a shared key see the above figure. The data is encrypted as follows: The CRC is generated as a checksum on the plain text. The IV is generated as a 128-bit random data field. The RC4 algorithm uses the concatenated IV/session key to encrypt the message along with the checksum. An exclusive or is performed between the encrypted message and checksum combination with the original message and checksum. The output of the exclusive or, referred to as the ciphertext, is pre-pended with the IV and then session key and transmitted over the air.

This means that a fairly patient hacker can determine *k* over a reasonable period of time. Once the hacker knows *k*, the security of the network has been compromised. Borisov et al, provide more details concerning the susceptibility of wireless communications outside of an 802.1X environment.

Clearly, if the keys could change dynamically then some of the inherent insecurity with WEP could be prevented. TLS provides for the dynamic key creation and a secure channel for which to communicate these keys. This is accomplished through the use of a private/public key encryption algorithm. The authenticator communicates with an authentication server. This authentication server may be a RADIUS (Remote Authentication Dial In User Service) or LDAP (Lightweight Directory Access Protocol) server or another server capable of providing the authentication.

The authentication server generates session keys during TLS negotiation. The authentication server communicates the keys to the authenticator and to the supplicant (via the authenticator) during the TLS transaction. Both the access point and the end-station are now aware of the session keys. The authenticator uses the session keys to create a dynamic WEP key.

The authenticator encrypts the WEP key using the session key and communicates it to the supplicant via the EAPOL_KEY message. Different keys are going to be generated each time the supplicant associates and authenticates itself with the access point. The supplicant decrypts the key using the session key and then communicates the key to the network interface driver. The network interface driver will use the key to encrypt and decrypt messages using the algorithm described above.

The EAPOL-Key message

The format of the EAPOL-key message is defined in 802.1X standard. The body of EAPOL-Key packet contains a Key-descriptor, and the format of the key descriptor depends on the descriptor type. Currently, only one descriptor type is defined—RC4. The format of the RC4 descriptor is shown below, along with a description of what each field contains when the WEP feature is enabled on the authenticator. The authenticator populates the fields and sends the packet to the supplicant.

	Octet number
Descriptor Type	1
Key Length	2-3
Replay Counter	4-11
Key IV	12-27
Key Index	28
Key Signature	29-44
Key	45 - EAPOL body length

Figure: RC4 key descriptor.

Descriptor Type The field is set to 'RC4 Key Descriptor Type', which is 1.

Key length The 2-byte field contains the key length in bytes (e.g., 5 for a 40 bit key).

Replay Counter The field contains 64-bit time stamp in NTP format. NTP timestamps are represented as a 64-bit unsigned fixed-point number, in seconds relative to 0h on 1 January 1900. The integer part is in the first 32 bits and the fraction part in the last 32 bits. In the fraction part, the non-significant low order can be set to 0.

Key IV The field contains 16-bytes long randomly generated vector. It is desirable that the vector generated is not repeated between AP reboots.

Key Index The field is one byte long. The low-order bits indicate the keys index when more than one key is being used. The high-order bit when on indicates that the key transmitted is a unicast key. When the bit is off, the key is a broadcast key.

Key Signature This field is a signature of all of the fields of the EAPOL packet, from and including the EAPOL protocol version field. The supplicant generates this independently and then compares its signature with the signature in this packet. The supplicant can believe that the packet is genuine and has not been tampered with.

Key The key field has to be empty (if configured so) or contain encrypted WEP key for STA.

AP Implementation

The Radius Server sends the EAP-Success message to the AP with the two secret keys. The AP turns around and sends an EAP-Success message to the Supplicant but there is no key involved (mandated by the standard).
The supplicant already knows the two keys needed to decrypt the EAPOL-key messages. EAPOL-Key messages are encrypted with the two secret keys resulting from authentication. During TLS authentication, the supplicant negotiates these keys with the Radius Server. The AP actually does not know until it is informed by the Radius Server. Next the AP sends EAPOL-key messages to the client to set the desired WEP keys on the client. The standard allows the AP to use the session key (which is a EAPOL-Key message with a null key value - the supplicant understands this to mean that it will choose one particular key out of the 2 secret keys as the WEP key) or the AP invents its own keys and sends them to the supplicant.

Setting a Dynamic WEP Key

When the supplicant receives the EAPOL-Key message it will decrypt the key and then communicate the key to the network interface driver. The supplicant's wireless LAN card will be reconfigured with the new encryption key through the network driver interface.

4. IEEE 802.1x

IEEE 802.1X is a recently issued standard for port based network access control to provide authenticated network access for Ethernet networks. It wasn't created specifically for wireless LAN but created to provide authenticated network access for Ethernet networks. This port-based, network access control uses the physical characteristics of the switched LAN infrastructure to provide a means of authenticating devices attached to a LAN port, and prevent access to that port if the authentication fails. Some of the key advantages of using 802.1x security are as follows:

1. We want to base authentication on client device independent items such as passwords (not equipment)
2. Clients should be able to communicate with RADIUS servers, possibly with Extensible Authentication Protocol (EAP), a RADIUS protocol extension.

3. Mutual authentication is better because it isolates rogue APs
4. WEP keys should be actually generated during authentication, rather than using static keys
5. WEP keys should be session based

IEEE 802.1x defines two logical access points to the LAN via a single physical authenticator LAN port: an uncontrolled port and a controlled port. The uncontrolled port allows uncontrolled exchange between the authenticator and other systems on the LAN regardless of the system's authorization state. The second logical access point denoted as the controlled port allows exchange between a system on the LAN and the authenticator services only if the system is authorized. The figure below shows an overview picture of 802.1x port authentication control:

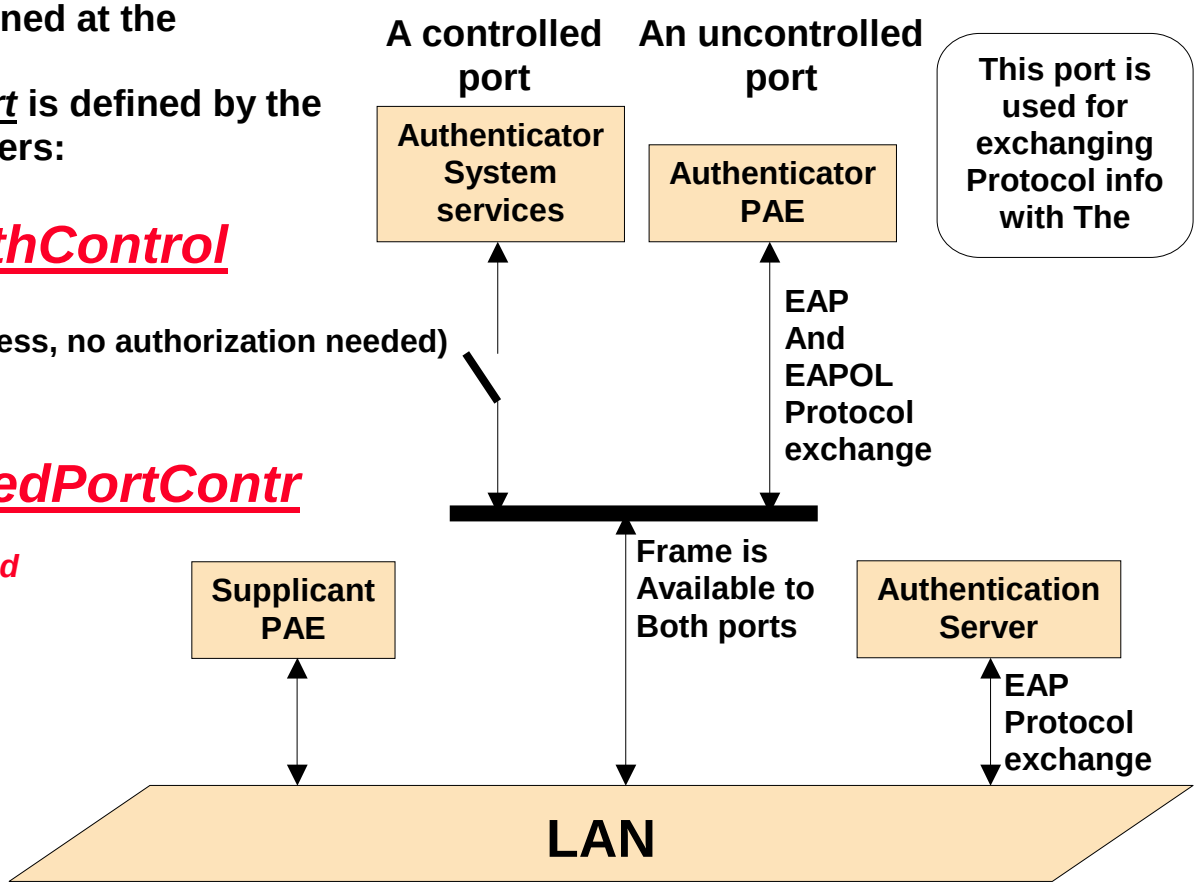
Two ports are defined at the authenticator.
The *controlled port* is defined by the following parameters:

SystemAuthControl

- ***Enabled***
- ***Disabled*** **(open access, no authorization needed)**

AuthControlledPortContr

- ***ForceUnauthorized***
- ***Auto***
- ***ForceAuthorized***



AuthControlledPortStatus

- **can be *Authorized***
- **can be *Unauthorized***

Port based network access control utilizes the physical characteristics of the switched LAN infrastructures in order to provide a means of authenticating devices attached to a LAN port, and for preventing access to that port in cases where the authentication process fails. A LAN port can adopt one of two roles with access control interaction: authenticator (AP) and supplicant (client PC or device). An authenticator is a port that enforces authentication before allowing access to services accessible via that port. The supplicant is a port that requests access to services accessible via the authenticator's port. The authentication server performs the authentication function to check the credentials of the supplicant on behalf of the authenticator and responds to the authenticator indicating whether or not the supplicant is authorized to access the authenticator's services. The authentication server may be a separate entity or its functions may be co-located with the authenticator.

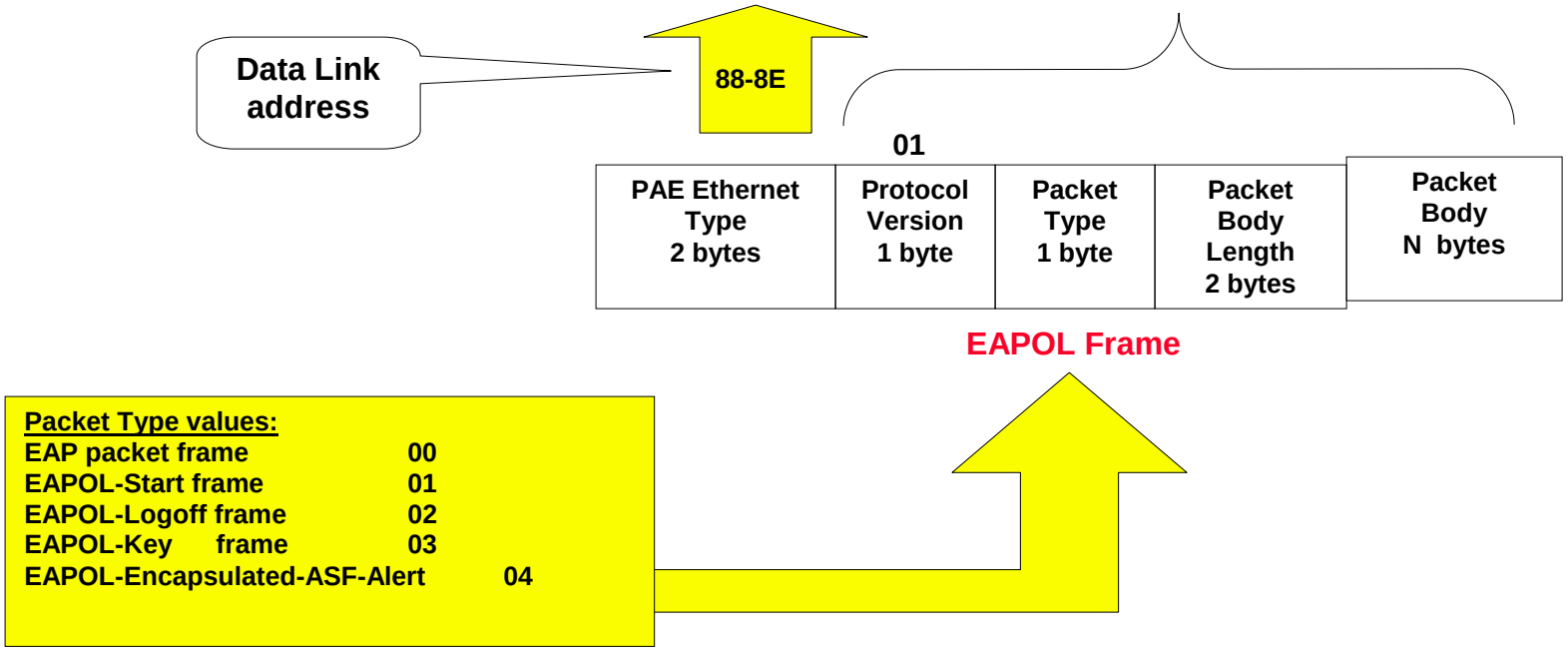
PAE, which stands for Port Access Entity is a LAN port, that can either be authenticator or supplicant. Authenticator is the one that gives the access to available port, while supplicant is the one that requests access to available service. Of course, association between them is needed prior to 802.1x authentication. Microsoft has implemented supplicant already implemented on their latest OS, WinXP. Microsoft is addressing wireless LAN security by taking this IEEE 802.1x standard that was in development for switched ethernet port-based access control and enhanced that to be applicable for 802.11. This is a basic authentication mechanism, specifying an Extensible Authentication Protocol (EAP), with additional capability to securely distribute the (WEP) encryption keys from the AP to the Stations. The ".1x Supplicant" in the client station uses EAPOL (EAP Over LAN) to transfer a higher layer authentication scheme to the ".1x Authenticator" in the AP. The Authenticator in the AP relays the EAP protocol to a RADIUS Authentication Server: EAP Over RADIUS.

Communication between PAEs is done using EAPOL (Extensible Authentication Protocol over LANs) exchanges.

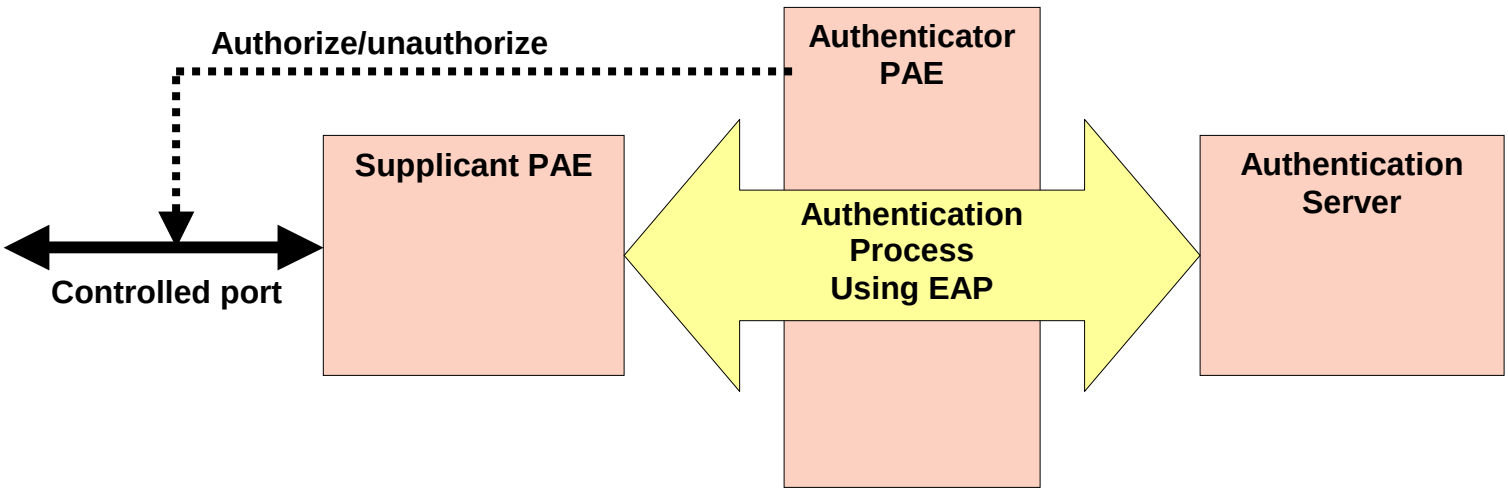
Shown below is details of EAP over LAN frame format:

Preamble 7 bytes	Start Frame Delimiter 1 byte	Destination Address 6 bytes	Source Address 6 bytes	Length/ Type 2 bytes	Data 46-1500 bytes	FCS 4 bytes

Ethernet 802.3 Frame

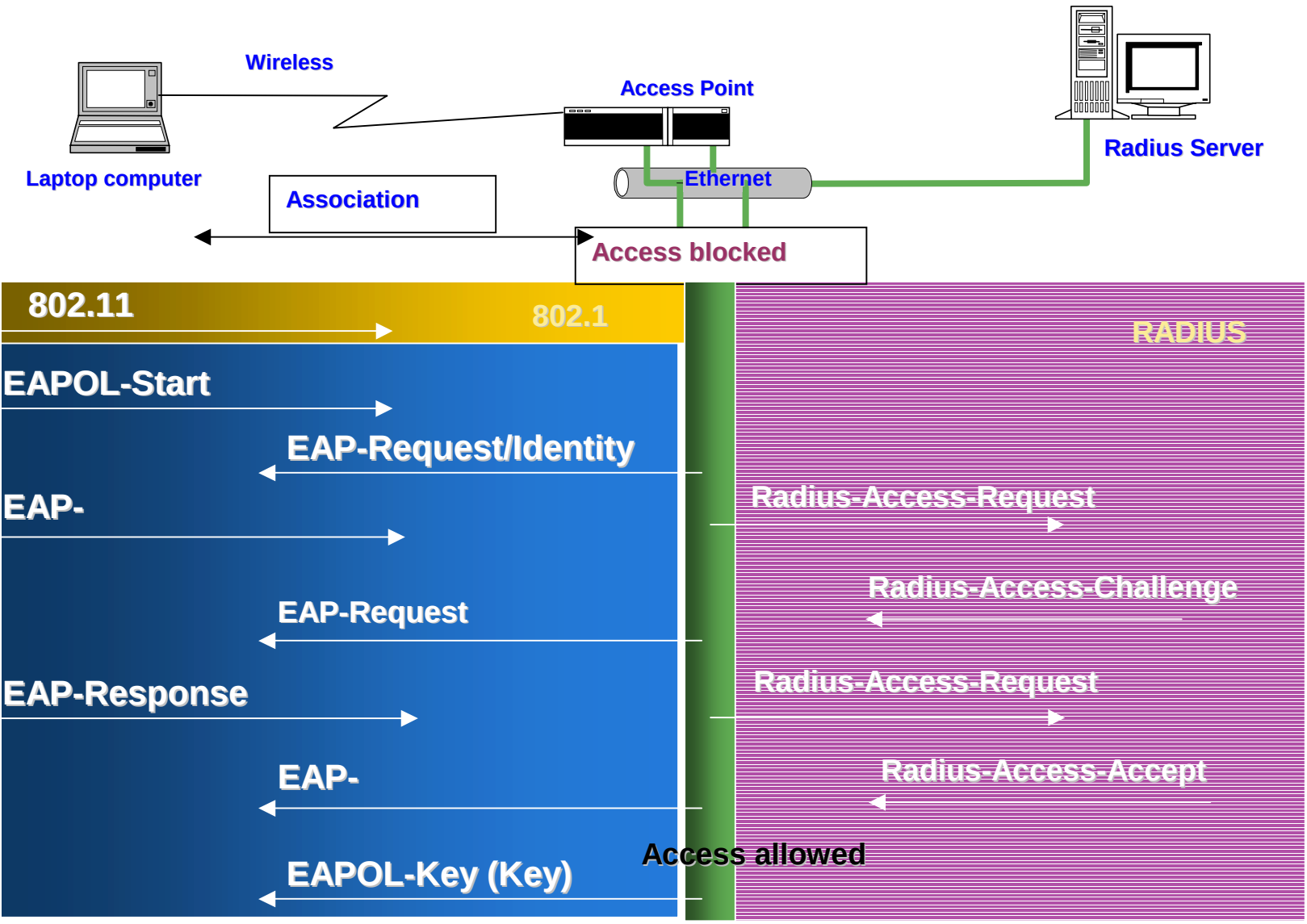


In Port Access Control of 802.1x, there only is connection between one supplicant and one authenticator. Supplicant must be able to access some services through the uncontrolled port prior to authentication (prior to DHCP and IP initialization). Below is figure of Port access control of 802.1x

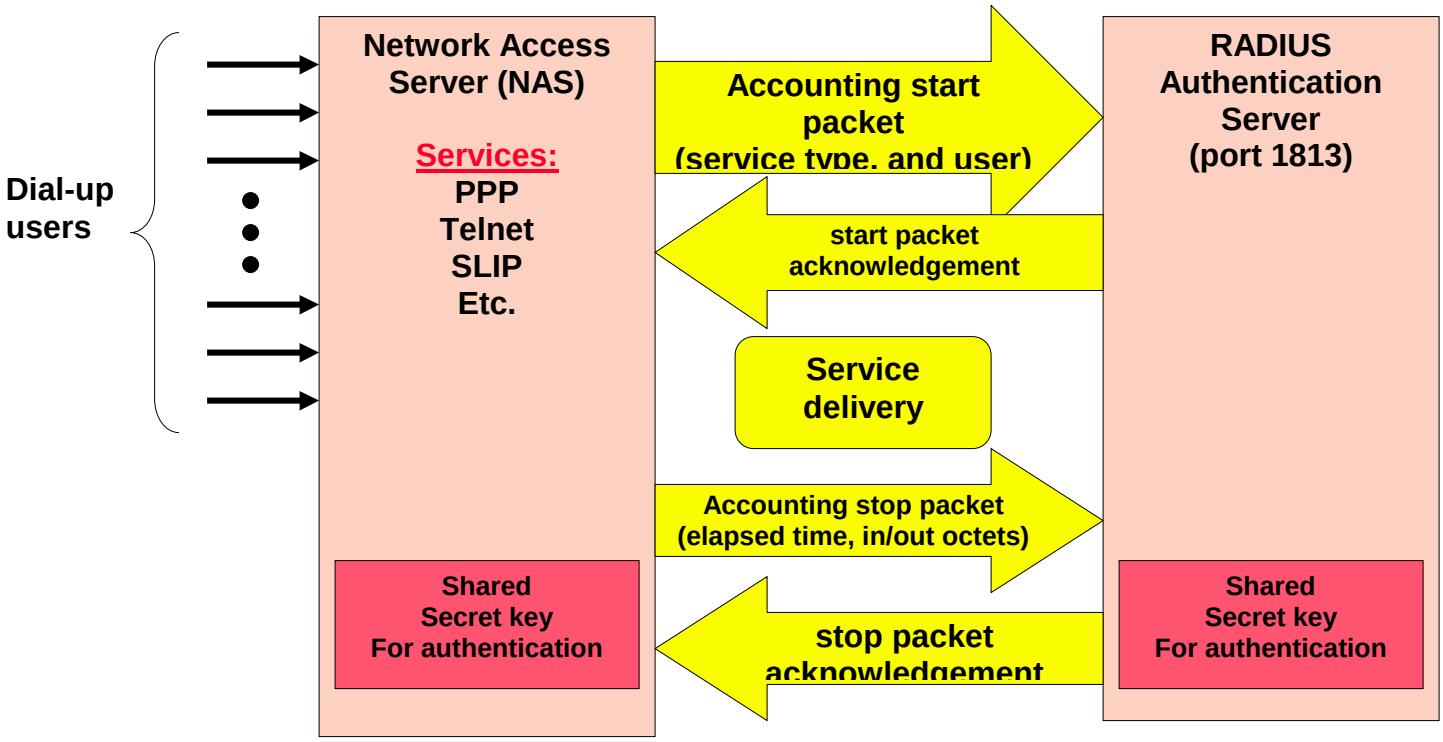


RAIDUS SERVER

Authentication server is also need to perform authentication functions, where it will check credentials of supplicant on behalf of the authenticator and respond back to the authenticator to indicated whether or not, supplicant is authorized to access the port requested. This is done by using a Remote Authentication Dial-In User Service (RADIUS) server for authenticating client credentials. RADIUS authenticates remote users against numerous back-end databases – allowing you to easily consolidate the administration of all your remote users, however they connect to your network. There are many RADIUS servers that can be used for authenticating a user. (i.e. Steel-Belted, NAVIS, Microsoft IAS, HP Unix RADIUS, Kerberos, Merit, etc.) An extension to the basic IEEE 802.1X protocol is required to allow a wireless access point to securely identify a particular client's traffic. This is done by passing an authentication key to the client, and to the wireless access point, as part of the authentication procedure. Only an authenticated client knows the authentication key, and the authentication key encrypts all packets sent by a client. Total picture of 802.1x on 802.11b from supplicant to Radius server and Handshake process is shown below:



When RADIUS is authenticating, each service constitutes a TCP/IP session. A user may have multiple sessions in parallel and each session has a separate start/stop accounting recorder (Acct-Session-Id). The process of RADIUS authenticating is shown below:



An IP packet's data field holds the RADIUS packet and the destination port field is 1813 for RADIUS delivery. The figure below shows the detail of the RADIUS packet format:

Code – the type of RADIUS packet 1 byte	**Identifier**– matches requests and replies (detects duplicates) 1 byte	**Length** – of the entire RADIUS packet 2 bytes	**Authenticator checksum**– called either the *Request Authenticator*, or the *Response Authenticator* 16 bytes	**Attributes** – Details about the acct-request or acct-response Type 1byte | Length 1byte | Value Var.

Acct-request=4
Acct-response=5

Request Authenticator is an MD-5 hash of The shared Secret, the Code, Identifier, Length, and request attributes fields

Response Authenticator is an MD-5 hash of The shared Secret, the accounting response code, Identifier, Length, and the initiating Request Authenticator fields

Type can be:
Acct-Status-Type = 40
Acct-Delay-Time = 41
Acct-Input-Octets=42
Acct-Output-Octets=43
Acct-Session-ID=44
Acct-Authentic=45
Acct-Session-Time=46
Acct-Input-Packets=47
Acct-Output-Packets=48
Acct-Terminate-Cause=49
Acct-Multisession-ID=50
Acct-Link-Count=51

Communication between the authenticator (AP) and authentication server is typically over an EAP connection in RADIUS. This is *not* part of 802.1x.
The AP must relay the EAP-TLS protocol between the RADIUS server and the Client device.
The RADIUS protocol must be supported between the AP and the RADIUS authentication server, per RFC 2138, and the IEEE 802.1X RADIUS Usage Guidelines, (draft-congdon-radius-8021x-11.txt). The EAP protocol as specified in RFC 2284 is used to negotiate the port-based authentication.
The Ether-type specified in the IEEE 802.1x standard (Draft 11) must be used to identify 802.1x EAP control packets.
The AP must inhibit data traffic from being forwarded to the wired Ethernet, a WDS link, or to another wireless STA prior to successful authentication.

If the AP receives an EAP-Start message from a STA, the AP transmits an EAP-Request (Identity) to the particular STA.

A STA must transmit an EAP-Start message on associating with a new AP.

A STA must transmit an EAP-Response (Identity) containing the user name in response to an EAP-Request (Identity). There may be cases where a device name and certificate are used (e.g. printers).

The wireless AP forwards the EAP-Response (Identity) message to a RADIUS server.

The RADIUS server sends an EAP-Request-TLS message to the AP.

The wireless AP forwards the EAP-Request from the RADIUS server to the STA.

The STA transmits an EAP-Response containing its credentials to the RADIUS server via the AP.

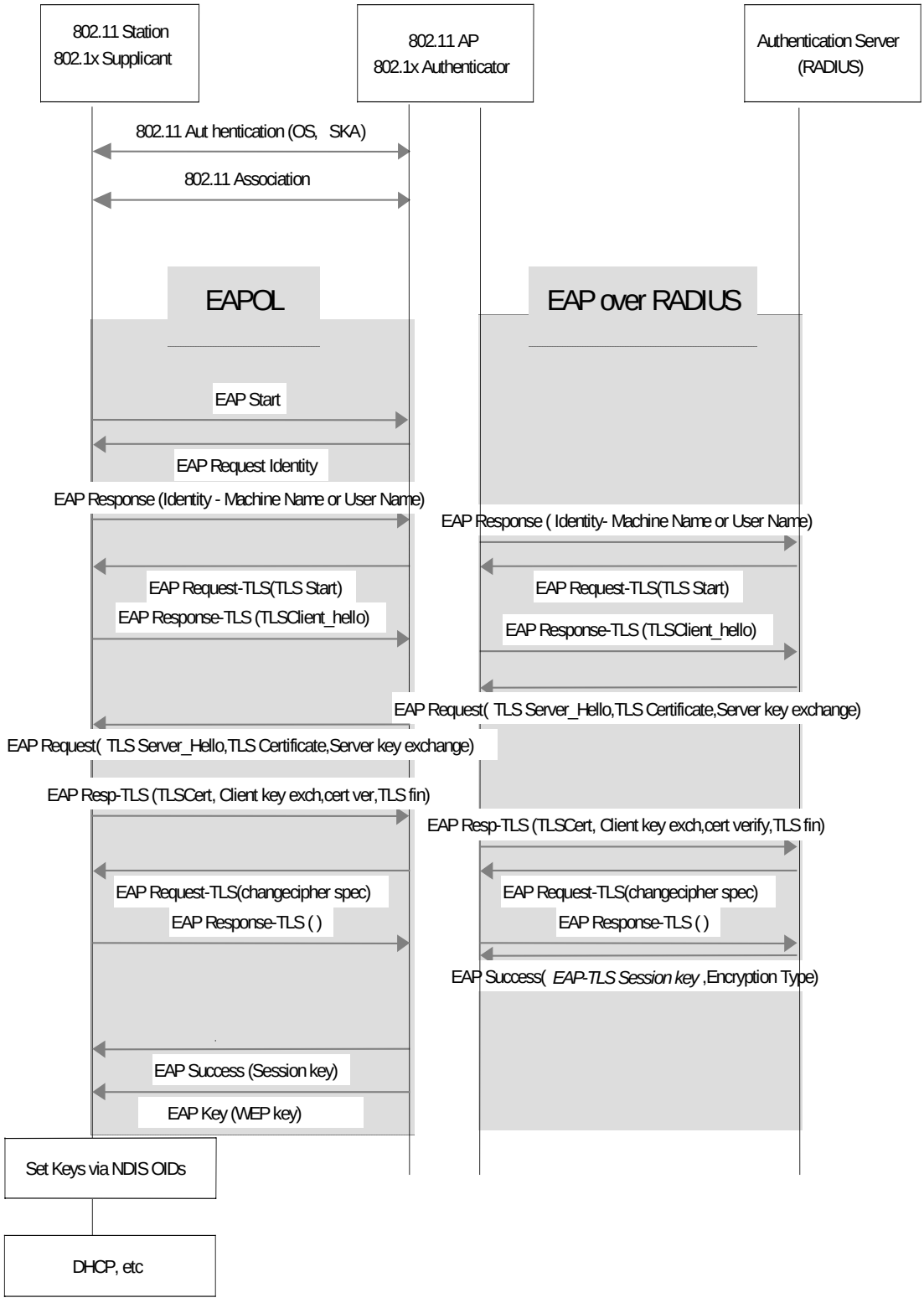
The AP forwards the STA's credentials to the RADIUS server.

The RADIUS server validates STA's credentials and sends a Success message to the AP.

The RADIUS server's response to the AP contains the STA message and the encryption key derived from the EAP-TLS session key.

The wireless AP forwards the success message to the STA after receiving the success indication from the RADIUS server.

Shown below is the outline out the EAP Protocol exchange with RADIUS that was discussed.


802.11 Station
802.1x Supplicant
802.11 AP
802.1x Authenticator
Authentication Server
(RADIUS)
802.11 Aut hentication (OS, SKA)
802.11 Association
EAPOL
EAP over RADIUS
EAP Start
EAP Request Identity
EAP Response (Identity - Machine Name or User Name)
EAP Response (Identity- Machine Name or User Name)
EAP Request-TLS(TLS Start)
EAP Response-TLS (TLSClient_hello)
EAP Request-TLS(TLS Start)
EAP Response-TLS (TLSClient_hello)
EAP Request(TLS Server_Hello,TLS Certificate,Server key exchange)
EAP Request(TLS Server_Hello,TLS Certificate,Server key exchange)
EAP Resp-TLS (TLSCert, Client key exch,cert ver,TLS fin)
EAP Resp-TLS (TLSCert, Client key exch,cert verify,TLS fin)
EAP Request-TLS(changecipher spec)
EAP Response-TLS ( )
EAP Request-TLS(changecipher spec)
EAP Response-TLS ( )
EAP Success(EAP-TLS Session key ,Encryption Type)
EAP Success (Session key)
EAP Key (WEP key)
Set Keys via NDIS OIDs
DHCP, etc

5. Present Market Comparison

Below is a quick chart of the security solution comparison:

Attribute	802.1X EAP-TLS	Cisco LEAP	802.11i
Encryption	Per frame RC4; Shared WEP key	Per Frame RC4; Shared WEP Key	WEP-2 and AES-OCB or AES-CBC MAC
Authentication Credentials	EAP-TLS Certificate based	EAP-Proprietary	EAP Type Negotiated; No EAP type specified as mandatory
Anonymity	Username in EAP-Identity message	Username in EAP-Identity message	Under Discussion Probably per-EAP type
Key Distribution	Automatic from AP	Automatic from AP	Automatic, Mechanism per-EAP type
Authentication Server	Microsoft Win2K with Active Directory	Cisco Server Only	As Per EAP type

Cisco LEAP solution is based on EAP but it is not a standard. This is Cisco's own proprietary scheme which does authentication and key distribution for a WLAN. Some of the significant weakness of this scheme include the following:

–authentication is not mutual: vulnerable to man-in-the-middle attack
–no anonymity protection: username goes over the air in the clear
–password has weak protection: weak hash algorithm used and is sent unprotected (dictionary attacks)
–needs proprietary Radius that supports LEAP
–use of one fixed WEP key in path from AP to client
–re-keying based on re-authentication only (inefficient)

6. Future of Wireless LAN Security

802.11i Security Extensions is another standard being formed by IEEE, which will define an Enhanced Security Network with improved Encryption and Entity Authentication. It will also improve major weaknesses of WEP while remaining backward compatible with existing hardware. Specific improvement to WEP will be done through random & longer IV and messaging authentication code. Emergence of 802.11i will further make 802.11 system more accepted in the market. Last thing worth mentioning is that it will provides a framework for incorporating new encryption, authentication, key exchange algorithms (evolution). Wireless Networking vendors will be moving forward to have support for Advanced Encryption Standard (AES), EAP Authentication Framework to support multiple authentication types, and evolvable to support Inter-network Roaming.

7. Conclusion

Granted that there are security issues with IEEE 802.11 wireless networking, but some of the concern has gotten out of proportion. Network administrators and companies hear this news and have been reluctant to deploy wireless networks; however the security limitation even without EAP security enhancement, 802.11 network is pretty secure if one configures the wireless network securely using 128-bit WEP along with closed system option so that network name is not broadcasted.

The freedom of wires and ease of network installation still makes IEEE 802.11-based, wireless network a very attractive solution. Now with the addition of IEEE 802.1X standards to IEEE 802.11 networks to improve the security beyond that of wired networks, wireless has and will become the way of the future. Things will only get better in this area of technology as industry improves other aspect of the technology such as ease-of-use, configuration, management, etc. On top of that, these security features can also be applied to other IEEE 802 networks to improve network-wide access security; for example, 802.3 Ethernet.

8. References

[1] Arbaugh, W., Mishra, A., “An Initial Security Analysis of the 802.1X Standard”, http://www.cs.umd.edu/%7Ewaa/1x.pdf .
[2] Aboba, B., Simon, D., “PPP EAP TLS Authentication Protocol,” IETF RFC 2716, http://www.ietf.org/rfc/rfc2716.txt
[3] Work in progress, Funk, P., Blake-Wilson, S., “EAP Tunneled TLS Authentication Protocol (EAP-TTLS),” http://ietf.org/internet-drafts/draft-ietf-pppext-eap-ttls-00.txt
[4] “Wireless LAN Authentication” white paper by Funk Software http://www.funk.com.
[5] Work in progress, Josefsson et al., “Protected EAP”, http://www.ietf.org/internet-drafts/
draft-josefsson-pppext-eap-tls-eap-02.txt
[6] Work in progress, Salgarelli, L., “EAP-Shared Key Exchange (EAP-SKE); A scheme for Authentication and Dynamic Key Exchange in 802.1X networks,” http://ietf.org/internet-drafts/draft-salgarelli-pppext-EAP-SKE-00.txt
[7] Work in progress, Haverinen, H., “GSM SIM Authentication and Key Generation for Mobile IP”, http://ietf.org/internet-drafts/draft-haverinen-mobileip-gsmsim-02.txt
[8] Work in progress, ” Carlson, J et al., “EAP SRP-SHA1 Authentication Protocol” http://ietf.org/internet-drafts/draft-ietf-pppext-eap-srp-03.txt
[9] Simpson, W., “PPP Challenge Handshake Authentication Protocol (CHAP)”, http://www.ietf.org/rfc/rfc1994.txt
[10] RFC Haller, N. and C. Metz, "A One-Time Password System", RFC 1938, May 1996. http://www.ietf.org/rfc/rfc1938.txt.
[11] Blunk, L., and J. Vollbrecht, "PPP Extensible Authentication Protocol (EAP)", RFC 2284, March 1998, http://www.ietf.org/rfc/rfc2284.txt.
[12] http://grouper.ieee.org/groups/802/11 [19] Rivest, R.,”The MD5 Message-Digest Algorithm” http://www.ietf.org/rfc/rfc1321.txt
[13] IEEE 802.11i, http://grouper.ieee.org/groups/802/11/.
[14] “Making IEEE 802.11 Networks Enterprise-Ready” By Arun Ayyagari and Tom Fout *Microsoft Corporation Published: May 2001*