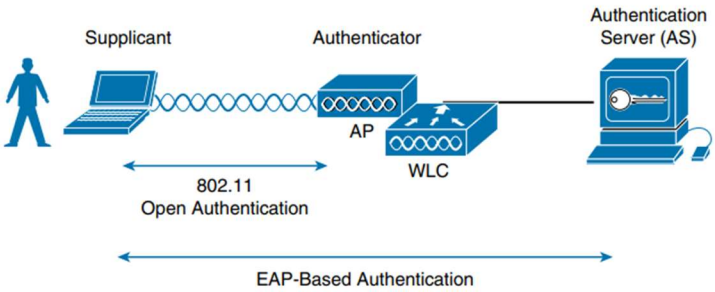
Wireless Security

The IEEE 802.1x standard defines a client-server-based access control and authentication protocol that prevents unauthorized clients from connecting to a LAN through publicly accessible ports unless they are properly authenticated. The authentication server authenticates each client connected to a switch port before making available any services offered by the switch or the LAN. Until the client is authenticated, 802.1x access control allows only Extensible Authentication Protocol over LAN (EAPOL), Cisco Discovery Protocol (CDP), and Spanning Tree Protocol (STP) traffic through the port to which the client is connected. After authentication is successful, normal traffic can pass through the port.

- **Supplicant:** The client device that is requesting access
- **Authenticator:** The network device that provides access to the network (usually a wireless LAN controller [WLC])
- **Authentication server (AS):** The device that takes user or client credentials and permits or denies network access based on a user database and policies (usually a RADIUS server)



	WEP	***WPA-Personal***	***WPA-Enterprise***	***WPA2-Personal***	***WPA2-Enterprise***	***WPA3-Pers/Ent***
Encryption	uses RC4 w/ WEP 24-bit IV 40-bit key / 128-bit key w/ TKIP	uses RC4 w/ TKIP 48-bit IV 128-bit key	uses RC4 w/ TKIP 48-bit IV 128-bit key	*AES-CCMP* 48-bit IV 128-bit key	*AES-CCMP* 48-bit IV 128-bit key	*AES-GCMP*
Authentication	Optional Shared Key OAS, SKA	PSK (Pre-Shared Key) 802.1x, EAP (RADIUS)	802.1x Various EAP-Types	PSK (Pre-Shared Key) 802.1x, EAP, RSNA	802.1x Various EAP-Types	PSK (*Personal*) 802.1x, EAP (*Enterprise*)
Integrity	Checksum / CRC	MIC (64-bit)	MIC (64-bit)	CBC-MAC 128-bit key	CBC-MAC 128-bit key	GMAC (Galois Msg Auth Code)

Table 28-2 Comparing WPA, WPA2, and WPA3

Authentication and Encryption Feature Support	WPA	WPA2	WPA3*
Authentication with **Pre-Shared Keys?**	Yes	Yes	Yes
Authentication with **802.1x?**	Yes	Yes	Yes
Encryption and MIC with **TKIP?**	Yes	No	No
Encryption and MIC with **AES and CCMP?**	Yes	Yes	No
Encryption and MIC with **AES and GCMP?**	No	No	Yes

* WPA3 includes other features beyond WPA and WPA2, such as Simultaneous Authentication of Equals (SAE), Forward secrecy, and Protected management frames (PMF).

Table 28-3 Review of Wireless Security Mechanisms and Options

Security Mechanism	Type		Type Expansion	Credentials Used
Authentication Methods	Open		Open Authentication	None, other than 802.11 protocol
	WEP		Wired Equivalent Privacy	Static WEP keys
	802.1x/EAP (Extensible Authentication Protocol)	LEAP	Lightweight EAP	Deprecated; uses dynamic WEP keys
		EAP-FAST	EAP Flexible Authentication by Secure Tunneling	Uses protected access credential (PAC)
		PEAP	Protected EAP	AS authenticated by digital certificate
		EAP-TLS	EAP Transport Layer Security	Client and AS authenticated by digital certificate
Privacy & Integrity Methods	TKIP		Temporal Key Integrity Protocol	N/A
	CCMP		Counter/CBC-MAC Protocol	N/A
	GCMP		Galois/Counter Mode Protocol	N/A