802.11a – do 54Mb/s, 5Ghz
802.11b – do 11Mb/s, 2,4Ghz
802.11g – do 54MB/s, 2,4Ghz

EAP umożliwia stosowanie oraz implementację różnorodnych metod uwierzytelniania w ujednolicony i niezależny od sprzętu pośredniczącego w komunikacji sposób. Architektura tego protokołu oparta jest o model klient/serwer. **+** obsługa różnorodnych metody uwierzytelniania, **+** istnieje możliwość negocjacji używanej metody uwierzytelniania, **+** ponieważ urządzenie dostępowe może pracować w roli pośrednika, możliwe jest wdrożenie **+** nowej (lub aktualizacja) metody uwierzytelniania, bez ingerowania w jego konfigurację, wymagana jest jedynie aktualizacja oprogramowania po stronie suplikanta i zewnętrznego serwera uwierzytelniania, **+** separacja pomiędzy urządzeniem dostępowym a zewnętrznym serwerem uwierzytelniania **+** ułatwia zarządzanie danymi poufnymi, takimi jak np. loginy i hasła użytkowników. **-** nie wszystkie implementacje PPP wspierają uwierzytelnianie z wykorzystaniem protokołu EAP, **-** sprzęt sieciowy (przełączniki, punkty dostępu) musi posiadać obsługę protokołu IEEE802, **-** ze względu na separacje urządzenia dostępowego od zewnętrznego serwera uwierzytelniania komplikuje się analiza zagadnień bezpieczeństwa.

Tłumienie wolnej przestrzeni jest definiowane jako strata sygnału na skutek sferycznego rozpraszania fal radiowych w przestrzeni. FSL = Lp (dB) = 106a(lub 100b) + 20log10 D, gdzie D – odległość

Wzmocnienie anteny: Ku(dB)=10logPwy/Pwe

WPA Personal – jeden klucz dla wszystkich, ręczna dystrybucja, WPA Enterprise – serwer RADIUS przydziela każdemu oddzielny klucz

Wzór Fresnela – obszar propagowania energii sygnału radiowego pomiędzy odbiornikiem a nadajnikiem. R=17,3*sqrt(d1*d2/d1d2*f)[m] w przestrzeni pozbawionej przeszkód.

WEP składa się z 2 częśći: wektora inicjującego o długości 24 bitów i klucza o długości 40 lub 104bit. Algorytm szyfrowania to RC4.

22Mhz – gdyż spektrum (2400-2483,5) jest podzielone na maksymalnie 14 kanałów (13) o tej szerokości. Tylko 3 mogą na siebie nie nachodzić.

W ramce występują 4 pola: odbiorca, nadawca, filtrowanie, opcjonalne

Wektor IV w WPA ma długość 48bitów, licznik ramek, zabezpiecza przed atakami typu replay

Metoda szyfrowania Podczas gdy WPA wersji pierwszej korzysta z TKIP/RC4 oraz Michael (MIC), WPA2 wykorzystuje CCMP/AES. WPA2 ma inne klucze dla szyfrowania danych i dla sumy kontrolnej