CCNP BCMSN Notes - Wireless Architecture and Design

Legacy Authentication Types **Open Authentication** No authentication is used; any client can associate to an AP. **Pre-Shared Key (PSK)** A pre-shared static Wired Equivalence Protocol (WEP) key authenticates the client to the AP. Extensible Authentication Protocol (EAP) Types EAP is an authentication framework originally developed for PPP authentication (RFC 3748). The wireless variants of EAP are defined in RFC 4017. **Lightweight EAP (LEAP)** LEAP (also known as Cisco EAP) is a Cisco-proprietary extension to EAP. Client and AP authentication is performed through a RADIUS server. Each authenticated client is assigned a unique WEP key. **EAP-TLS** EAP-TLS (defined in RFC 2716) uses Transport Layer Security (TLS) and relies on digital certificates for authentication. Every client and AP must have a valid digital certificate to be authenticated. Each authenticated client is assigned a unique WEP key. **Protected EAP (PEAP)** PEAP is similar to EAP-TLS (it also relied on TLS), but only the authentication server is required to have a digital certificate; this certificate is used to authenticate the server to clients. Clients are authenticated using MS-CHAPv2. EAP Flexible Authentication via Secure Tunneling (EAP-FAST) EAP-FAST establishes a secure tunnel between the client and the authentication server using a Protected Access Credential (PAC). The PAC can be assigned from a PAC server or generated dynamically. Wi-Fi Protected Access (WPA) Types **WPA** First-generation WPA was based on draft 802.11i. WPA utilizes Temporal Key Integrity Protocol (TKIP); WEP keys are incremented per-packet, and regenerated on reauthentication. Some form of EAP or a preshared key is used for the initial authentication exchange. Message Integrity Check (MIC) is used to provide message integrity (hashing). **WPA2** WPA2 was developed from the finalized 802.11i standard. WPA2 relies on Advanced Encryption Standard (AES) for encryption, which requires a hardware upgrade from WEP/WPA. TKIP is supported for backward-compatibility with WPA. Proactive Key Caching (PKC) can be used to allow a client to roam between APs without reauthenticating to each. Cisco Compatible Extensions (CCX) Cisco developed CCX as a certification process for ensuring compatibility between devices:
**   CCXv1** - Basic 802.11 compatibility, 802.1x for LEAP, multiple SSIDs **   CCXv2** - WPA, 802.1x for PEAP, fast roaming with CCKM, RF scanning **   CCXv3** - WPA2, 802.1x for EAP-FAST, Wi-Fi Multimedia QoS (802.11e)
**   CCXv4** - Cisco NAC, VOIP call admission control, VOIP metrics, enhanced roaming, RFID functionality Roaming APs with overlapping coverage areas should be configured to operate on non-overlapping channels (1, 6, and 11 for 802.11b/g). Vendor-specific roaming algorithms determine when a wireless client will decide to roam. Clients can scan channels for other APs in two ways:
**   Passive scanning** - A client only listens for beacon frames **   Active scanning** - A client actively transmits probe requests A client must disassociate with the current AP before it can associate with another. WLAN Design **AP Cell Size** A larger cell has the potential to support more clients than is desired. Effective transmitter power determines the cell size. Antenna type determines the cell shape. **Channel Layout** Cells should be laid out in a honeycomb fashion, preventing dead space and overlapping channels; this can be accomplished with only three non-overlapping channels.