

**Description of the Cisco Aironet 1130AG Access Point –**

* Cisco Aironet 1130AG Series is a product that provide high-capacity, high-security, enterprise-class features in a discreet , office-class design that is delivering WLAN access with the lowest total cost of ownership .
* The Cisco Aironet 1130AG Series is available in two versions : - a lightweight version , an autonomous version that can be field-upgraded to lightweight operation and a single band 802.11g version for use in regulatory domains that do not allow 802.11a/5 GHz operation .
* The Cisco Aironet 1130AG Series can be configured to support the OfficeExtend solution for secure , wireless teleworking . More , Cisco Aironet can also be configured to support Enterprise Wireless Mesh (WMN is a communication network made up of radio nodes organized in a mesh topology ) providing wireless connectivity for indoor areas that are difficult or impossible wire .

**Capabilities of Cisco Aironet 1130AG Access Point –**

* The Cisco Aironet 1130AG Access Point use radio and network management features for simplified deployment , along with build-in omnidirectional antennas that provide WLAN coverage for offices and similar RF ( Radio Frequency ) environments .
* With high-performing dual IEEE 802.11 and 802.11g , the Cisco Aironet 1130AG Series provides a combined capacity up to 108 Mbps to meet the needs of growing WLANs .
* When configured with LWAPP ( Lightweight Access Point Protocol ) , the Cisco Aironet can automatically detect the best-available wireless LAN controller .
* The Cisco Aironet 1130AG Series delivers optimal value for officers and similar environments .
* Cisco Aironet1130AG Series hardware-accelerated AES ( Advanced Encryption Standard ) encryption supports enterprise-class , government grade secure over the WLAN without compromising performance .
* Autonomous or unified Cisco Aironet 1130AG Series Access Points support management frame protection for the authentication of 802.11 management frames by the wireless network infrastructure . This allows the network to detect spoofed frames from access points or malicious users .
* If an access point detects a malicious attack , an incident will be generated by the access point and reports will be gathered on the Cisco wireless LAN controller .