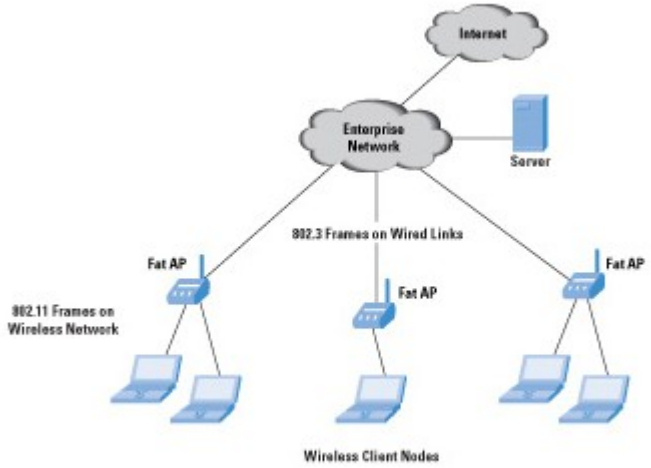
Fat, Thin, and Fit APs

In a managed WiFi network, consisting of multiple access points and the access controller, the level of data control and management the AC has to furnish depends upon the level of autonomous operation the APs have.

To understand this further it is useful to look at the functions performed by the three common types of access point. First off Fat APs, which form the core of an autonomous architecture. Then there are Thin APs which only have the simple basics of self operation so all data flow and organisation as well as management is handled by the AC. In between the Fat and Thin AP in functionality is the Fit AP.

Fat Access Points

Below shows an example of an autonomous network with Fat access points.



The AP is an addressable node in the network with its own IP address on its interfaces. It can forward traffic between the wired and wireless interfaces. It can also have more than one wired interface and can forward traffic between the wired interfaces—similar to a Layer 2 or Layer 3 switch. Connectivity to the wired enterprise can be through a Layer 2 or Layer 3 network.

It is important to understand that there is no “backhauling” of traffic from the Fat AP to another device through tunnels. This aspect is important and is addressed when discussing the other AP types. Typically Fat APs can also be used as stand alone access points which can operate in the absence of any controller device.

In a network based around an access controller management of the AP is typically done through a protocol such as the *Simple Network Management Protocol* (SNMP) or the *Hypertext Transfer Protocol* (HTTP) for Web-based management and a *Command-Line Interface* (CLI). To manage multiple APs, the network manager has to connect to each AP through one of these management schemes. Each AP shows up on the network map as a separate node. Any aggregation of the nodes for management and control has to be done at the *Network Management System* (NMS) level via the controller or sometimes via a software based NMS application.

Since Fat APs have fully autonomous operation then a managed Fat AP/AC scenario typically has at least all of the functionality that would be present in stand alone APs such as *Access Control Lists*

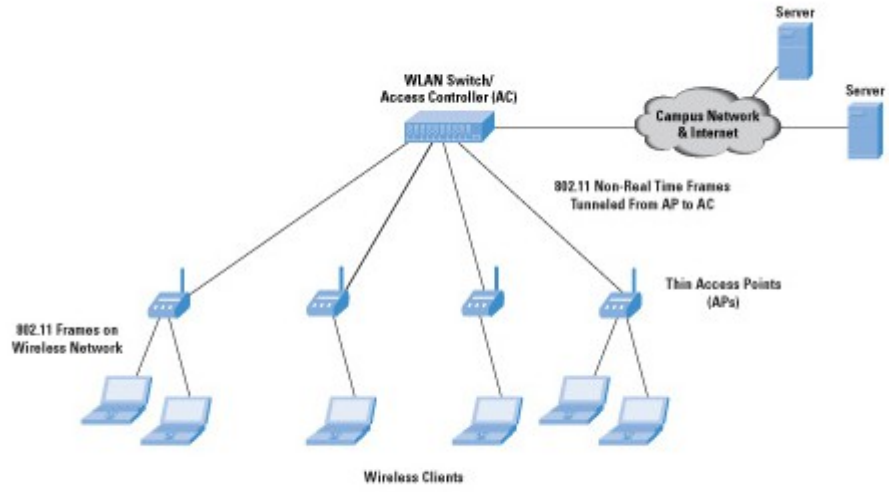
(ACLs), *Quality of Service* (QoS)-related functions, VLAN support, band-steering, bandwidth control, etc...

The downsides of Fat APs are complexity and cost. Fat APs tend to be built on powerful hardware and require complex software which adds to costs.

A Fit AP/AC installation still uses a controller at the back end for control and management functions but the APs are a slightly scaled-down version of the Fat AP. This simplifies the AP construction with a significant change in costs.

Thin Access Points

As their name indicates, Thin APs are intended to reduce the complexity of the hardware of APs. Thin APs are often known as "intelligent antennas," in that their primary function is to receive and transmit wireless traffic. They backhaul the wireless frames to a controller where the frames are processed before being switched to the wired LAN (see below).



The APs use a (typically secure) tunnel to backhaul the wireless traffic to the controller. In their most basic form, Thin APs do not even perform WLAN encryption such as *Wired Equivalence Privacy* (WEP) or *WiFi Protected Access* (WPA/WPA2). This encryption is done at the controller—the APs just transmit or receive the encrypted wireless frames, thereby keeping the APs simple and avoiding the necessity to upgrade their hardware or software.

The protocol between the AP and the controller for carrying the control and data traffic is typically proprietary. Also, due to the higher work load, the controller generally needs to be based on a more powerful hardware platform than required for a Fat AP installation. Another important requirement is that the connectivity and tunnel between the AP and the AC should ensure low delay for packets between those two entities. With Thin APs, QoS enforcement and ACL-based filtering are handled at the controller along with all other apsects of the wifi connectivity.

Fit Access Points

Fit APs are gaining in popularity in that they try to combine the advantages of both Fat and Thin APs. So a Fit AP provides the wireless encryption while using the AC for the actual key exchange. This approach is used for newer APs that use the latest wireless chipsets supporting WPA2. The management and policy functions reside on the controller that connects to multiple APs through

tunnels. In comparison, with a Thin AP setup all of this data encryption and handling would have to be handled by the AC.

Also, Fit APs are able to provide additional functions such as DHCP relay for the station to obtain an IP address through DHCP. In addition, Fit APs can perform functions such as VLAN tagging based on the *Service Set Identifier* (SSID) that the client uses to associate with the AP (when the AP supports multiple SSIDs).

Exactly how the various tasks of data flow, management, and control are split between AP and AC varies between manufactures. For example whether the wireless 802.11 MAC functions are handled by the AP or the AC (these include management and control frame processing). With Local MAC architectures these functions are handled by the AP. With a Split MAC architecture those functions which require real time handling (such as beacon generation, probe transmission and response, and control frame processing) are processed by the AP with less critical functions such as authentication and deauthentication, association and reassociation, bridging between Ethernet and Wireless LAN, etc, being handled by the AC.