

The Care and Feeding of SSIDs

What is an SSID?

An SSID (Service Set Identifier) is a sequence of characters that uniquely names a wireless LAN, allowing clients to connect to the desired network when multiple independent networks are present. APs (access points) advertise their presence up to 50 times per second by broadcasting 'beacon' frames that carry the SSID. Clients can discover SSIDs by passively scanning for these beacons sequentially across all channels. Alternatively, they can send out 'probe' frames on all channels to search actively for an AP with an SSID that matches the one they are probing for. Having located one or more APs with the right SSID, the client then sends an 'associate request' frame to the one offering the highest signal strength. The SSID is the only human-readable way an AP can advertise its presence to potential users.

'Hiding' the SSID

Some APs can be configured to hide their SSID by not including it in their beacons, treating it as a 'password' to WLAN access rather than as a community label. However, beacon frames are not the only route by which SSIDs are disclosed. For example, it is legitimate to construct a zero-length SSID, which is called a broadcast SSID. If an AP receives a probe request with a broadcast SSID from a client, it returns its actual SSID – i.e. the broadcast SSID probe is a mechanism that triggers all APs within range to announce their SSIDs. The SSID is therefore easily discovered, even from 'protected' APs. So, although placing a broadcast SSID in the beacon frame is sufficient to conceal the network identity from the casual WLAN user using only the network discovery tools built in to their operating system, the false sense of security provided by a 'hidden' SSID added to the support load incurred through making the user manually set the SSID suggests that this practice is of questionable utility.

'Any' Port in a Storm

APs may be configured in two system authentication modes, 'open' or 'closed'. Closed system authentication requires that the exact SSID be entered in the client configuration settings to permit association. Open system authentication behaves in the same way as a closed network, but additionally honours the convention that clients with their SSID set to 'any' are also permitted to associate.

Virtual APs: Multiple SSIDs per AP

Enterprise-class APs increasingly support multiple SSIDs. This feature logically divides the access point into several 'virtual APs' within a single hardware platform, conserving spectrum and maximizing infrastructure flexibility in multi-provider environments (such as airports, stations etc.). Unfortunately, ways to implement this feature are not yet standardized between different AP and NIC (Network Interface Card) vendors, resulting in interoperability problems.

Given multiple SSID support, different policies and functions may be assigned for each SSID, increasing the flexibility and efficiency of the network infrastructure. For example:

- **VLAN Injection.** You can assign an SSID to a VLAN, and the AP injects client devices using that SSID into the relevant VLAN. This enables the separation of wireless applications based on security and performance requirements.
- **Maximum number of client associations.** You can set the number of users that can associate via a particular SSID, which makes it possible to control usage of particular applications. This can help provide a somewhat limited form of bandwidth control for particular applications.
- **Multiple providers could share the same physical infrastructure,** and select the services they wish to provide in terms of rates, security mechanisms, etc. Each provider could manage their own users without interfering with other providers and customers could discover any of the offered networks without needing to preconfigure their clients.

Well Known SSIDs

APs are often preconfigured to run 'out of the box'. These default settings are typically at the lowest security level, to provide the easiest access for further configuration. Knowledge of the factory default SSIDs of common wireless hardware can therefore be useful in monitoring your wireless environment in order to detect unsecured 'rogue' APs: if you detect such an SSID (e.g. 'tsunami', 'linksys') then it is reasonable to infer the presence of an AP deployed in its most basic configuration, and thus a potential security risk.

In the education sphere, LIN (location independent networking) services are provided via the **eduroam** SSID. This SSID has been widely adopted as an international standard to indicate wireless services that participate in roaming agreements between institutions, such that staff or students from one site may use their home credentials to access resources on other sites. In the UK, the principal eduroam-enabled roaming system is JANET Roaming

Further Reading

- 802.11i draft paper on virtual APs:
<http://www.drizzle.com/~aboba/IEEE/>
- Eduroam in the Netherlands:
<http://www.eduroam.nl/en/>
- JANET Roaming:
<http://www.ja.net/roaming>
- The Care and Feeding of SSIDs, by Mark O'Leary [an expanded and more technical version of this factsheet]:
<http://www.ja.net/development/wireless/documents/care-and-feeding-of-ssids.pdf>