The care and feeding of SSIDs

Mark O'Leary

July 2005

Contents

What is an SSID?

An SSID (Service Set Identifier, sometimes also called the ESS Name) is a sequence of characters that uniquely names a wireless LAN, allowing clients to connect to the desired network when multiple independent networks operate in the same physical area.

More formally, each set of wireless devices communicating directly with each other is called a BSS (Basic Service Set) – for example, an AP and the clients associated with it form a BSS. Several BSSs can be joined together to form a single logical wireless LAN segment, referred to as an ESS (Extended Service Set) – i.e. the number of APs (access points) and associated clients that form a departmental LAN. An SSID is simply the case-sensitive 1-32 byte alphanumeric name given to each ESS, and works in a manner analogous to NetBIOS Scope functions to logically segment a network. It is an information element that may be incorporated into various management frames of the 802.11 protocols.

In default configuration, APs advertise their presence up to 50 times per second by broadcasting 'beacon' frames that carry the SSID (along with the time, AP channel, capabilities and supported rates, etc). 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 actively search for an AP with an SSID that matches the one they are probing for. An AP receiving a probe that carries an SSID it supports replies with an associate response frame, also containing the SSID. Having thus 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.

So, a wireless device user instructs their client card to join a network by specifying the SSID of that network. It is up to the 802.11 driver, firmware and hardware to decide which AP to associate with. If multiple APs are advertising the same SSID then the client will pick the most

appropriate one. Some vendors make that decision based on information contained in the beacon frames, but the choice of AP is still up to the client. The SSID is the only available method to instruct a client about which network it should join. (Although it is possible with some cards/drivers to specify the broadcast SSID (see below) of a particular AP, that method is cumbersome and does not allow a client to roam between APs.) Furthermore, the SSID is the only human-readable way an AP can advertise its presence to potential users.

‘Hiding’ the SSID

It is legitimate to construct a zero-length SSID, which is a termed a broadcast SSID. If a client sends a probe request that carries a broadcast SSID, the AP returns its actual SSID in the probe response. Thus the broadcast SSID probe is a mechanism that allows the client to trigger all APs within range to broadcast their SSIDs.

As a security measure, some APs can be configured to send a broadcast SSID in their beacon frames instead of sending their actual SSID(s). This approach views the SSID as a password to WLAN access rather than in its intended role as a community label. However, it is not possible to keep an SSID value secret in this way because the SSID is carried in more than just the beacon frames, as we have seen above. It is also required in probe requests and responses, and association/reassociation requests. A broadcast SSID could be used in any of these frames, but in practice at least the associate and reassociate frames must always contain the SSID, since if they were to use a broadcast SSID then there would be no restrictions as to which clients can join the WLAN. (In normal operation, if the SSID in these frame types does not match the SSID configured in the AP then the AP rejects the association.) The SSID is therefore regularly exposed and may be ‘sniffed’ (i.e. discovered by analysing packets captured using a similar client radio). Trivially, by sending a faked disassociate frame to an active client, it can be forced to send out the SSID in a reassociate request, so it does not even require the capture of a volume of traffic to discover the SSID of a WLAN ‘protected’ in this way.

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, but even this low level of security comes at a price. There may be a high frequency of probe requests and responses, triggered by changes in the local wireless environment such as new clients starting up, interference, and low signal strength as well as just the initial association and roaming events due to mobility. This represents a substantial networking overhead and reduces the efficiency of the WLAN.

Overall, the false sense of security provided by a ‘hidden’ SSID, added to the support load incurred through mandating that the SSID must be set correctly by the user rather than discovered, suggests that this practice is of questionable utility. It should not be considered a valid means of securing a wireless network.

‘Any’ Port in a Storm

Access Points 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. If a client sends out a probe carrying the SSID of

‘any’, all open authentication APs in range will respond and the client can simply select the channel with the best signal strength. It is thus a function of the AP configuration as to whether the use of ‘SSID=any’ on the client results in association. However, if SSID broadcast functionality is disabled by setting a broadcast SSID in the beacon frame then clients cannot connect to the AP with an ‘any’ SSID. Instead, the correct SSID must be specified for association to proceed.

Virtual APs: Multiple SSIDs per AP

To have one AP with multiple IDs goes against the concept of the SSID as originally intended in 802.11b, since it is a *service set* identifier and one cannot have more than one actual service set on one channel at one time. However, there is increasing demand for enterprise-class APs that support multiple SSIDs. Such functionality 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.

Virtual APs emulate the operation of physical APs at the MAC and IP layers, but not at the radio frequency layer, since all the virtual APs must use the same channel that the single physical radio is set to. There are a number of technical issues to overcome to achieve virtual AP functionality. A full implementation requires:

- Multiple SSID/capability advertisement in beacon frames
- Support for probe frame discovery of advertised SSIDs
- Multiple VLAN support
- Multiple RADIUS configurations.

Also desirable would be determination of the target SSID prior to association (for routing of pre-authentication traffic) and separate IP addresses per virtual AP (e.g. to allow multiple RADIUS shared secrets, and to facilitate a virtual MIB instance per virtual AP). Possible ways of accomplishing this are:

1. **Multiple SSIDs per Beacon, Single Beacon, Single SSID.** The AP uses a single SSID and sends a single beacon, but the beacon and probe response frames include multiple SSID information elements. This is not explicitly prohibited by IEEE 802.11-1999, and allows discovery of multiple SSIDs, but it is incompatible with many existing clients, cannot support different capability sets for each SSID or multiple capability sets within an SSID, and does not support pre-authentication routing.
2. **Single SSID per Beacon, Multiple Beacons, Single SSID.** The AP only uses a single SSID, but sends multiple beacons, each with a single SSID information element. The AP responds to probe requests for supported SSIDs (including a request for the broadcast SSID) with a probe response including the capabilities corresponding to each SSID. This approach can support different capability sets for each SSID and allows discovery of multiple SSIDs, but some existing drivers will over-write previous advertisements with the new one, and this method cannot support multiple capability sets within an SSID or pre-authentication routing.
3. **Single SSID per Beacon, Single Beacon, Single SSID.** The AP uses a single broadcast SSID and sends a single beacon; each beacon or probe response contains only one SSID information element. Only the capabilities corresponding to the primary SSID are sent in the beacon and in response to a probe request for the broadcast SSID.

The AP responds to probe requests specifically for secondary SSIDs with a probe response including the capabilities specific to that SSID. This approach is compatible with existing clients and does support different capability sets for each SSID. However, it does not allow discovery of secondary SSIDs (i.e. requires pre-configuration), cannot support multiple capability sets within an SSID, and does not support pre-authentication routing.

4. **Single SSID/Beacon, Multiple Beacons, Multiple SSIDs.** The AP uses multiple SSIDs. Each beacon or probe response contains only a single SSID information element. The AP sends beacons for each virtual AP that it supports at the standard beacon interval, using a unique SSID for each one. The AP responds to probe requests for supported SSIDs (including a request for the broadcast SSID) with a probe response including the capabilities corresponding to each SSID. Such an approach would be compatible with existing clients, supports different capability sets for each SSID and multiple capability sets within an SSID, allows discovery of multiple SSIDs and supports pre-authentication routing.

This whole area was not addressed in IEEE 802.11-1999, so multiple approaches have been taken by AP vendors and different assumptions made by NIC (Network Interface Cards) vendors, resulting in interoperability problems.

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

- **VLAN Injection.** An SSID can be assigned to a VLAN, and the AP injects client devices using that SSID into the relevant VLAN (by dot1q tagging). This enables the separation of wireless applications based on security and performance requirements.
- **Maximum number of client associations.** The number of users that can associate via a particular SSID can be set, which makes it possible to control usage of particular applications. This can help provide a somewhat limited form of bandwidth control for particular applications.

By means of multiple SSID support, a number of providers could announce their own SSID over 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. (Additionally, multiple virtual APs could advertise the same SSID but a different capability set, allowing different security levels, for example.)

Well Known SSIDs

As a technology aimed at the SOHO market, 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. Unfortunately, users often do not appreciate the security issues associated with wireless networking, and given a working configuration have little motivation to change it. A knowledge of the factory default SSIDs of common wireless hardware can therefore be useful in monitoring a wireless environment in order to detect unsecured ‘rogue’ APs: if a wireless surveying exercise detects 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 student 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 eduroam.

Choosing SSIDs

The following guidelines may help select an appropriate SSID for a wireless network:

- SSIDs should be meaningful to humans (numeric codes and the like should be avoided).
- SSIDs should be consistent across multiple AP deployments (either a common service name, or a consistently applied naming scheme).
- When participating in national or international schemes, their agreed common SSID should be adopted.
- Where possible, SSIDs should indicate sources of further information on the service (i.e. a name that reflects the ownership of the network, or possibly even uses a URL as an SSID to point directly to further data).

Further Reading

- • *802.11i draft paper on virtual Aps:* http://www.drizzle.com/~aboba/IEEE/ [1]
- • *Eduroam in the Netherlands:* http://www.eduroam.nl/website_new/index.php?lang=en [2]

Links
[1] http://www.drizzle.com/%7Eaboba/IEEE/
[2] http://www.eduroam.nl/website_new/index.php?lang=en