**WLAN**

In [IEEE 802.11](https://en.wikipedia.org/wiki/IEEE_802.11) [wireless local area networking](https://en.wikipedia.org/wiki/Wireless_LAN) standards (including [Wi-Fi](https://en.wikipedia.org/wiki/Wi-Fi)), a **service set** is a group of wireless network devices which share a *service set identifier* (*SSID*)—typically the [natural language](https://en.wikipedia.org/wiki/Natural_language) label that users see as a network name. (For example, all of the devices that together form and use a Wi‑Fi network called *Foo* are a service set.) A service set forms a logical network of nodes operating with shared [link-layer](https://en.wikipedia.org/wiki/Data_link_layer) networking parameters; they form one [logical network segment](https://en.wikipedia.org/wiki/Logical_link_control).

* The 802.11 standard describes different service sets.
* A service set describes how a group of wireless devices communicate with each other.
* Proti ti router er wi-fi ar je akta individual name thake take bola hoy SSID.
* Each service set uses the Same Service Set Identifier (SSID).

**Advantages of WLANs**

The most obvious advantage of a WLAN is that devices can connect wirelessly, eliminating the need for cables. This allows homes and businesses to create local networks without wiring the building with Ethernet. It also provides a way for small devices, such as smartphones and tablets, to connect to the network. WLANs are not limited by the number of physical ports on the router and therefore can support dozens or even hundreds of devices. The range of a WLAN can easily be extended by adding one or more repeaters. Finally, a WLAN can be easily upgraded by replacing routers with new versions — a much easier and cheaper solution than upgrading old Ethernet cables.

### Disadvantages of WLANs

Wireless networks are naturally less secure than wired networks. Any wireless device can attempt to connect to a WLAN, so it is important to limit access to the network if security is a concern. This is typically done using wireless authentication such as [WEP](https://techterms.com/definition/wep) or [WPA](https://techterms.com/definition/wpa), which encrypts the communication. Additionally, wireless networks are more susceptible to interference from other signals or physical barriers, such as concrete walls. Since LANs offer the highest performance and security, they are still used for many corporate and government networks.

There are many setup:

**1. IBSS (Independent Basic Service Set) :** With an Independent Basic Service Set (IBSS), two or more wireless devices connect directly without an access point (AP).

An *independent BSS* (*IBSS*), or *ad hoc network*, is created by peer devices among themselves without network infrastructure.[[6]](https://en.wikipedia.org/wiki/Service_set_(802.11_network)#cite_note-FOOTNOTEIEEE_Std_802.11-2012%C2%A7_4.10.4,_pp._88%E2%80%9390-6) A temporary network created by a cellular telephone to share its Internet access with other devices is a common example. In contrast to the stations in an infrastructure-mode network, the stations in a [wireless ad hoc network](https://en.wikipedia.org/wiki/Wireless_ad_hoc_network) communicate directly with one another, i.e. without a dependence on a distribution point to relay traffic between them.[[7]](https://en.wikipedia.org/wiki/Service_set_(802.11_network)#cite_note-FOOTNOTEIEEE_Std_802.11-2007%C2%A7_5.6,_p._41-7) In this form of peer-to-peer wireless networking, the peers form an *independent basic service set* (*IBSS*).[[8]](https://en.wikipedia.org/wiki/Service_set_(802.11_network)#cite_note-FOOTNOTEIEEE_Std_802.11-2007%C2%A7_5.21,_p._25-8) Some of the responsibilities of a distribution point—such as defining network parameters and other "beaconing" functions—are established by the first station in an ad-hoc network. But that station does not relay traffic between the other stations; instead, the peers communicate directly with one another. Like an infrastructure BSS, an independent-BSS also as a 48-bit MAC-address-like identifier. But unlike infrastructure BSS identifiers, independent-BSSs identifiers are not necessarily unique: the *individual/group* bit of the address is always set to 0 (individual), the *universal/local* bit of the address is always set to 1 (local), and the remaining 46 bits are randomly generated.

Atar jonno jekono akta device SSID tah advertise korbe and onno device join korbe.

IBSS is not a popular solution because speed kom thake, atar network weak thake, and insecuire thake.

**2. Infrastructure Mode :** With infrastructure mode, we connect all wireless devices to a central device, that called an access point (AP). All data goes through the AP. The 802.11 standard describes different service sets. Let’s take a look.

* Basic Service Set (BSS): With a Basic Service Set (BSS), wireless clients connect to a wireless network through an AP. A BSS is what we use for most wireless networks. The idea behind a BSS is that the AP is responsible for the wireless network.

Each wireless client advertises its capabilities to the AP, and the AP

grants or denies permission to join the network. The BSS uses a single

channel for all communication. The AP and its wireless clients use the

same channel to transmit and receive.

Amra previous Wi-Fi e chapter bibinno doroner standard porsilam jekon a,b,g,n . ai standard gulo BSS advertise kore tokhon AP buje je hae thik ase ami ata accept korbo or na o korte pari. Tokhon akta password ar mathdome AP sathe join hote pare / password na thakle join hote parbe nah.

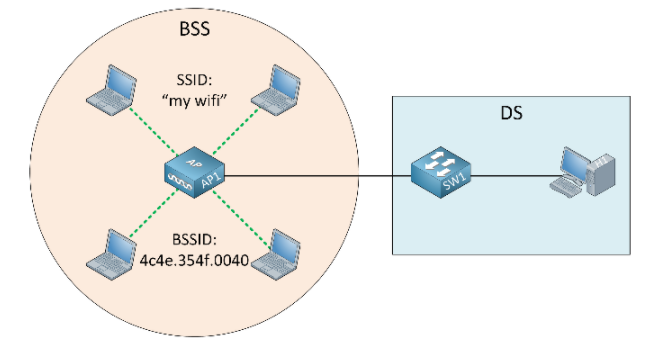
|  |  |
| --- | --- |
| * The SSID is the “my wifi” name of the wireless network, and it doesn’t have to be unique. * The AP also advertises the Basic Service Set Identifier (BSSID). This is the MAC address (48 bits) of the AP’s radio, a unique address that identifies the AP. All wireless clients have to connect to the AP. This means the AP’s signal range defines the size of the BSS. We call this the Basic Service Area (BSA). | BSS.PNG |

When a wireless device wants to join the BSS, it sends an association request to the AP. The AP either permits or denies the request. When the wireless device has joined the BSS, we call it a wireless client or 802.11 station (STA).

All traffic from a wireless client has to go through the AP even if it is destined for another wireless client.

Everything has to go through the AP because the AP is our central point for management, and it limits the size of the BSS. The AP’s signal range defines the boundary of the BSS.

* Distribution System (DS): A BSS is a standalone network with a single AP. In the pictures above, there is no connection with a wired network. Most wireless networks, however, are an extension of the wired network. An AP supports both wired and wireless connections. The 802.11 standard calls the upstream wired network the distribution system (DS). The AP bridges the wireless and wired L2 Ethernet frames, allowing traffic to flow from the wired to the wireless network and vice versa.



Each wireless network has a unique BSSID. The BSSID is based on the MAC address, so most vendors (including Cisco) increment the last digit of the MAC address to create a unique BSSID.

Even though we have multiple wireless networks, they all use the same underlying hardware, radios, and channels. If you have an AP with multiple radios, then it’s possible to assign wireless networks to different radios. For example, you could use one wireless network on the 2.4 GHz radio and another one on the 5 GHz radio.

* Extended Service Set (ESS) : An *extended service set* (*ESS*) is a wireless network, created by multiple access points, which appears to users as a single, seamless network, such as a network covering a home or office that it too large for reliable coverage by a single access point. It is a set of one or more infrastructure basic service sets on a common [logical network segment](https://en.wikipedia.org/wiki/Logical_link_control) (i.e. same IP subnet and VLAN).

A BSS uses a single AP. This might not be enough because of two reasons:

1. Coverage: A single AP’s signal can’t cover an entire floor or building. You need multiple APs if you want wireless everywhere.
2. Bandwidth: An AP uses a single channel, and wireless is half-duplex. The more active wireless clients you have, the lower your throughput will be. This also depends on the data rates you support. A wireless client that sits on the border of your BSA might still be able to reach the AP, but can only use low data rates. A wireless client that sits close to the AP can use high data rates. The distant wireless client will claim more “airtime,” reducing bandwidth for everyone.

|  |  |
| --- | --- |
| To create a larger wireless network, we use multiple APs and connect all of them to the wired network. The APs work together to create a large wireless network that spans an entire floor or building. The user only sees a single SSID, so they won’t notice whether we use one or multiple APs. Each AP uses a different BSSID, so behind the scenes, the wireless client sees multiple APs it can connect to. We call this topology with multiple APs, an Extended Service Set (ESS). | DS.PNG |

* Mesh Basic Service Set (MBSS): A mesh basic service set (MBSS) forms a self-contained network of mesh stations that share a mesh profile. Each node may also be an access point hosting its own basic service set, for example using the mesh BSS to provide Internet access for local users. From the point of view of a wireless client, an [IEEE 802.11s](https://en.wikipedia.org/wiki/IEEE_802.11s) [wireless mesh network](https://en.wikipedia.org/wiki/Wireless_mesh_network) appears as a conventional infrastructure mode topology, and is centrally configured as such. The formation of the mesh's BSS, as well as wireless traffic management (including path selection and forwarding) is negotiated between the [nodes](https://en.wikipedia.org/wiki/Node_(networking)) of the mesh infrastructure. The mesh's BSS is distinct from the networks (which may also be wireless) used by a mesh's redistribution points to communicate with one another.

If you want to provide a wireless network for a large area, like a city, then it’s not easy to connect each AP to a wired network. Instead, you could build a mesh network, also known as a Mesh Basic Service Set (MBSS). With a mesh network, we bridge wireless traffic from one AP to another. Mesh APs usually have multiple radios. One radio is for backhaul traffic of the mesh network between APs; the other radio is to maintain a BSS for wireless clients on another

channel. At least one AP is connected to the wired network; we call this the Root AP (RAP). The other APs are Mesh APs (MAP) and are only connected through the wireless backhaul.