ITRAINONLINE MMTK
ACCESS POINT CONFIGURATION HANDOUT

Developed by: IT +46
Based on the original work of:
Onno W. Purbo and Sebastian Buettrich

Table of Contents

1. About this document

These materials are part of the ItrainOnline Multimedia Training Kit (MMTK). The MMTK provides an integrated set of multimedia training materials and resources to support community media, community multimedia centres, telecentres, and other initiatives using information and communications technologies (ICTs) to empower communities and support development work.

1.1 Copyright information

This unit is made available under the Creative Commons Attribution-ShareAlike 2.5 License. To find out how you may use these materials please read the copyright statement included with this unit or see http://creativecommons.org/licenses/by-sa/2.5/.

1.2 Degree of difficulty

The degree of difficulty of this unit is "Basic" with some additional "Advanced" parts. All "Advanced" parts are marked with a red frame to emphasise the higher level of difficulty of that section.

2. Introduction

This unit provides a general methodology for installing and configuring wireless access points and routers. Instead of focusing on "which button to press", we aim to provide an understanding of what each setting implies and when and why a certain setting is needed. The methodology follows the OSI model with main focus on the physical and the link layer.

Additionally, a graphical web based step-by-step process of access point configuration is provided in Appendix 1.

3. Before You Start

Independent of which hardware you are using or what network topology you might want to set up, there is a set of general guidelines that you should always keep in mind.

1. Read the manual of the access point and get to know the device and its default settings.
2. Consider the physical installation placement (access to power, antennas, temperature, humidity etc.). See "Site Survey" for further information.
3. Plan the network (TCP/IP) before you start and make a drawing of the topology. Planning includes knowing your ISP's or LAN settings including DNS, etc.
4. Make sure that you have all documentation and material (physically, not only online), so you can work even if you are disconnected during the process.
5. Take notes about every step you take in the configuration process, especially when changing IP addresses, network settings and passwords.
6. Make sure that you have all necessary hardware needed (PC/laptop with wireless and Ethernet interfaces)
7. Make sure that you have all necessary software needed such as:
    • TCP/IP software tools (ping, route)
    • Vendor specific software (firmware upgrades, drivers, etc.)
    • Software to measure/detect wireless signals (Kismet, Netstumbler)

4. Installing hardware and firmware

The first step of the configuration process is to install the hardware, connect the access point to your computer and (optionally) update the firmware. This section give you an overview of the general physical layout of an access points and how to physically install the device.

4.1 Physical installation

There are typically two different parts of the access points that you should pay attention to:

1. Status LEDs (diodes)[1]
2. Radio and Ethernet Interfaces

A set of LEDs is normally found on top of the access point indicating the status of the device. The LEDs typically indicate with flashing or steady (green or red) light the following parameters:

1. Power to the access point
2. Active ports
3. Internal error
4. Ethernet connection (uplink)

The LEDs can give you highly valuable information while troubleshooting your network. We strongly suggest you to carefully study the meaning of each diode in the reference manual of your access point before starting the setup process.

The basic interfaces of a wireless access point are.

1. Ethernet: often called WAN (connection to Internet) or LAN (connection to LAN). A "pure" access point (wireless bridge) has only one Ethernet port. An access point with more than one Ethernet port is normally a Wireless Router/Gateway.
2. Radio/Antenna(s): Wireless connection to clients

More advanced wireless devices can be equipped with two or more wireless interfaces (two or more radios).

On one of the rear sides, we can typically find the Ethernet interfaces together with a few other functionalities.

1. Power input (12V, 5 V or 3.5 V DC): connect to DC power source.
2. Reset button: Used to restore default settings
3. LAN Connectors (RJ45): connect to LAN
4. WAN port (RJ45): connects to a DSL, cable modem or any upstreams provider for uplink connectivity
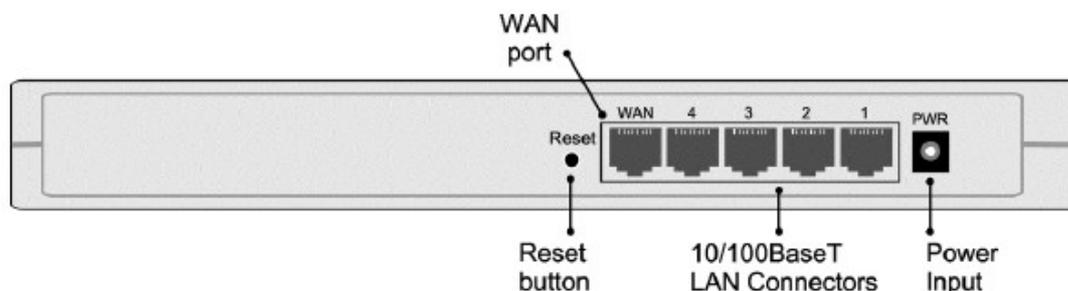

Image 1: A typical setup of connectors and adapters on the rear end of an access point (wireless router).

---

1   LED= A light-emitting diode

Furthermore, an access point is equipped with a (pair of) antenna(s) that can be built in or attached to the cover of the access point. The external antennas can normally be adjusted to fit a specific implementation.

4.2 Updating Firmware

The firmware is a software that has been written into the ROM (read-only memory) and become a permanent part of the device. One can say the firmware is a hard-software. The firmware will remain in the ROM memory after the device has been switched off. The BIOS program that controls every computer at start up is also a "firmware".

Vendors update the firmware of their products continuously to offer the latest configuration and correct reported bugs. Always update the access point to the latest "stable" firmware before you start to configure it and check for updates periodically.

4.3 Connect your computer to the device

To configure the access point, you need to connect your PC or laptop to it. This can be done *wired* or *wireless*.
It is highly recommendable to start the configuration using a wired connection and later, once basic settings are in place and you feel more confident with the configuration process, switch to wireless.

The wired connection can be done using:
1. Ethernet cable via HTTP
2. Ethernet using vendor specific software based on SNMP
3. Serial cable (Null modem) using HyperTerminal or other serial communication program (if the access point has a Serial Port)

Among the three options, the most common is to connect via Ethernet cable using HTTP. This way of configuring the access point is platform independent and only requires a web browser. Be aware, that the User Interface (UI) will look different from vendor to vendor and from model to model. They change constantly and you will never find two of the same kind. However, they all contain the same basic elements. Also be aware that not all the vendors refer to the same "concepts" with the same words.

The basic concepts are introduced below:

To be able to communicate with the access point, you need to belong to the same IP subnet. Look in the reference manual for the default IP address of the access point and change your own IP address accordingly. Thereafter, open a browser window and proceed with the configuration though the web based interface.

There are also "proprietary" setup utilities for access points configuration which you install on your computer in order to setup a wireless device. They are normally based on a protocol known as SNMP. (See Troubleshooting Unit)

The third option, using a serial cable, can be considered as your "backup plan" when things have gone wrong. This option implies that you need to have physical access to the device, and can hence not be done by "anyone". Serial cable is typically used as way to reconfigure the access point when you have forgotten the password and do not want to reset to default settings. Normally, you can access the access points via the serial interface without knowing the password (or you can set up a non-password via the Serial Cable).

5. Configuring hardware following the OSI model

At first glance, access point configuration might look fairly complex, judging by the thickness of the reference manual. Normally, a great amount of settings are available and it can be difficult to distinguish the basic settings from the mode advanced settings.

A "pure"[1] access point only needs two settings:
1.   SSID name
2.   Channel number

However, it is often convenient to set other parameters. Many optional parameters refers to security in terms of encryption and restricted access, but are of course important if you want to secure the connection.

Below follows a theoretical approach to hardware configuration that follows the OSI model and puts emphasise on what each setting actually does and why it is needed. We strongly believe that to understand, WHY a certain configuration is important and WHAT a certain parameter implies, is essential for building high quality wireless networks.

As we know by now, wireless networking is restricted to the first two layers of the OSI model, the physical and the link level. Since an access point is a wireless device, nothing else than a "wireless hub", its pure wireless settings are all affecting the first two OSI layers.

If the access points supports routing and NATing, they will also includes settings related to the OSI Layer 3: IP layer.

5.1 The Physical Layer

The parameters of an access points that affect the physical layer are the following:

5.1.1 Channel Number

When setting the channel of an access point, you determine the range of frequencies (Ghz) that the device will operate in. Before you set the channel, you should scan the frequency range of interest with a software like "Netstumbler" or similar, to avoid using the same channel as other networks (if present). By doing so, you will ensure a more "idle" frequency spectrum for your network.
For IEEE 802.11b networks, use channels 1, 6 or 11 to ensure enough frequency separation to avoid conflicts. For 802.11a networks there is no risk of overlapping channels, so just make sure surrounding IEEE 802.11a access points are operating in different channels than the one you select.
Some new access points have a feature that automatically sets the channel based on idle frequency by scanning the spectrum and finding out which ones that are already in use.
See unit "Site Survey" for further information.

5.1.2 Transmit power

The higher the transmit power is, the larger coverage range the access point will give you. If you aim to archive as large coverage as possible, the transmit power should be set to the highest value. For many countries the upper legal limit it 100mW (20dB), while in others (many African countries) that upper limit is 1-3 W.

Not all the access points will allow you to set up the output power. Notice that the upper legal limit of power needs to be calculated considering the gain of the antenna that you use. (See Radio Link Calculation)

---

1   By "pure" we mean an Access Point that acts a wireless bridge with NO routing capabilities. The access point does not provide NAT, DHCP etc.

If you instead aim for increasing the overall capacity of the wireless network by adding access points close together, then the power should be set to to a lower value in order to decease overlap and potential interference. Alternatively, you will like to place antennas adequately to minimize inter-AP interference.

5.1.3 Speed or capacity

In some access points, it is possible to select the preferred speed of operation (11, 5.5, 2 or 1 Mbps for IEEE 802.11b). By doing so, the modulation technique of the data transfer is being changed.

As default, set the speed to the highest possible value. If you are building a very long link and experience problems with packet loss, you can try to reduce the speed in order to have a more robust signal.

5.2 The Link layer

The parameters of an access points that affect the link layer are the following:

5.2.1 Operational Modes

The mode of the access point should not be confused with the two basic "radio" modes of any wireless card, which are infrastructure and ad-hoc.

The mode of an access point refers to what kind of tasks it performs. The denotation of "mode" can many times be confusing since different vendors uses different names to describe an operational mode of a product.
You should keep in mind that a pure *access point* only performs tasks related to *radio functionality* such as *bridging*. If a so called "access point" deals with *IP related tasks*, such as *routing and NATing*, we are talking about a *wireless router*. The different modes mainly differ in weather the access point performs bridging or routing/NATing.

The section below describe a set of typical "modes'" that you will find in access points (or wireless routers). Note that the name of the mode can differ from vendor to vendor.

Access Point Bridging (alt. Access Point Mode)
The access point works as a pure bridge between a router and wireless clients. No routing or NATing takes place in the access point. This is the simplest configuration mode for an wireless access point.

Gateway
The access point acts as a wireless router between a LAN and a set of wireless clients by performing routing or NATing to its clients. The access point can obtain an IP address from the upstream provider by means of DHCP. The access point can deliver IPs by DHCP to its clients.

Point-to-Point bridge (alt. Repeater mode)
Two access points are used to bridge TWO wired networks. No NATing is performed in the access points as it simply passes on data packets.

Point-to-Point routing (alt. Wireless Bridge Link)
The access point is used as a wireless router between two separate LAN's.

Wireless Ethernet adapter (alt. Wireless Client mode)
This mode is used to connect any computer that does not support wireless adapters. By connecting an access point to such a device via Ethernet or USB, the access points can be used "as a wireless adapter".

5.2.2 SSID (Service set identifier)

The SSID is the name of the wireless LAN and is also attached to all "beacon" packets sent by the access points[1]. The SSID is a case sensitive text string that accepts up to 32 alphanumeric characters and it is used to during the "association" process to a wireless network. The association process is equivalent to the action of "plugging a cable" into the wall.

Clients that want to communicate with a certain access point, must use the SSID during the "association" process (see Client Installation for further information).

The SSID of an access point is by default broadcasted (beacon) to announce its presence. That means that anyone with a wireless adapter can "see" your network in terms of your SSID. If no extra security mechanism in terms of encryption (WPA) or authentication (MAC filtering, captive portal) has been implemented in the access point or the network, anyone can associate with your access point and reach the network behind it.

Many access points offer the possibility to turn off the broadcasting of the SSID and in that way make it possible to "hide" the network to the public. This trick can be used to improve the wireless network security against average computer users. However, for advanced users it is a weak form of wireless network security since with the right tools, you can monitor and capture certain packets of the wireless network and in that way find the SSID.

5.2.3 Media Access Control

There are some advanced settings in access points that can be particularly relevant for congested (crowded) networks. Those parameters are for example Beacon interval, RTS/CTS and fragmentation.

Beacon interval
The beacon interval is the amount of time between access point beacon transmissions. The default value for this interval is generally 10ms, which implies that 10 beacons are sent every second.

This value gives you sufficient support in terms of mobility within an office environment. If you need support for higher mobility, you can increase the beacon interval. Decreasing the beacon interval results in a reduced overhead in the network but it is likely that roaming between base stations will not work seamlessly.

We recommend you not to change this value unless you have very good reasons to do so.

---

1   More information about SSID: http://www.issa-uk.org/downloads/presentations/issa-uk/wp_ssid_hiding.pdf.

Request-to-send (RTS) / Clear-to-send (CTS)

RTS/CTS is the method used by IEEE 802.11 wireless networks to reduce collisions caused by "hidden nodes" (See "Advanced Wireless Networking"). In brief, it is a method to grant access to use the medium which involves a handshaking process between an access point and a wireless node.

RTS/CTS introduces Collision Avoidance in CSMA/CA and hence, makes the access method more robust. At the same time, it adds unavoidable overhead to the network.

The RTS/CTS works as following. A node that wants to send data initiate the handshake with the access points by sending a RTS frame. The access points receives the RTS and responds with a CTS frame if the medium is idle. When the node receives the CTS, it starts to send its data. As all the nodes must be able to listen to the access point, the CTS frame will reach all nodes connected to it. The CTS frame includes a time value that the other nodes must wait until they send any RTS frame. A completed RTS/CTS handshake will ensure that the node can send its data without being corrupted by frames sent by other nodes.

If there is only a few clients in the wireless network and all of them can "see" each other, the RTS/CTS option should be switched OFF. Using RTS/CTS in this case would only introduce overhead by including RTS/CTS frames and decrease the total throughput.

If there is a chance of hidden nodes in the network, you should consider using RTS/CTS. In this case, RTS, CTS will both introduce overhead in terms of RTS/CTS frames but might also reduce the overall overhead in terms of fewer retransmissions of data frames. The questions is which factors that is the larger one? Do you introduce more overhead than you reduce? To find our, you need to measure the packet loss rate (on TCP level) for both options.

Fragmentation

The IEEE 802.11 standard includes an optional feature that allows radio based NICs and access points to fragment data frames intro smaller pieces to improve performance in presence of interference or poorly covered areas.

By sending smaller frames, the risk of collisions with other frames are less likely. This results in increased reliability of frame transmission (but higher overhead).

The fragmentation value, normally between 256-2048 bytes, can be controlled by the user. The fragmentation effect will take place when the access point or the wireless nodes tries to send a frame with greater size than the fragmentation threshold.

Just like the RTS/CTS function, you should first monitor the network and estimate the amount of retransmissions caused by collisions. If the level of collisions is high, then consider changing the fragmentation threshold.

In the case of less than 5% collisions, do not use the fragmentation option since the overhead of the fragmentation frames would introduce more overhead than the "non-existing" collisions would reduce.

5.2.4 Access Control through MAC filtering

MAC filtering implies that you allow only a limited set of known MAC addresses to connect to the access point. This is a very weak security measurement but can be used in combination with other more advanced solutions.

An advanced user can easily capture packets that is coming from/to the network and find out which MAC addresses that are granted access. Thereafter, it can change the its own MAC address to one of the accepted ones and "fool" the access point by pretending to be someone else.

5.2.5 Encryption (WEP, WPA)

WEP (Wired Equivalent Privacy) is an **old** encryption protocol implemented in most access points nowadays. Although WEP has proven to have great weaknesses and is no longer considered to be a safe option for

encryption, it is frequently used among average users.

WEP uses the RC-4 40-bit encryption algorithm to scramble all data before transmission between access points and clients. Many vendors add proprietary encryption features to their software and raise the encryption level up to 128 bits.

The WEP configuration done in the access point must always be reflected in the client side. Make sure that your client device support the encryption protocol, authentication type and key length that you configure your access point to run.

If you choose to enable WEP, always remove the default WEP keys that are provided by the vendor and set your own private keys. If you use the 64-bit key (40 bit as actual key), you must enter a key consisting of 10 hexadecimal characters (0-9, a-f or A-F). The 128-bit key, that provides higher security, consists of a hexadecimal 26 characters long string.

Remember! The current alternative to WEP is WPA (Wi-Fi Protected Access), which is the encryption protocol that was designed to address the problems of WEP. WPA2 is the second generation of WPA which is based on the IEEE 802.11i amendment.

Still many access points on the market today (2006) supports only WEP by default. Normally, you will find that a firmware update of the access point and the wireless client to WPA is available. Check the vendor website for firmware upgrades. To improve the network security of your network by supporting WPA encryption, the following items needs firmware upgrade:

1. Wireless access points

2. Wireless network adapters

3. Wireless client programs (drivers, management tools etc)

For more information regarding wireless encryption see "Wireless Security".

5.2.6 Restricted access through authentication

Restricted access to a network by means of authentication can be done by using a Radius Authentication server. If a Radium Authentication server is implemented, the access point acts as a "Radius client" and must be aware of the database settings in the Radius server.

As a part of the original IEEE 802.11 standard MAC functions, access points offer open system authentication and sometimes even share key authentication. Since neither one of these authentication systems have proven to be secure, many access points nowadays includes IEEE 802.1x mechanisms for allow authentication of users via an external authentication server.

The topic of authentication goes beyond the scope of this unit and will not be further discussed.

5.2.7 End-to-end encryption

End-to-end encryption is the most secure way to protect transfer of valuable data. VPN (Virtual Private Network) offers an end-to-end encryption service and is supported by many access points today. In the case of implementing a VPN, the access point enable VPN Pass-through via PPTP/IPSec.

VPN is beyond the scope of this unit and we will not be further discussed.

5.3 The IP layer

Strictly speaking, the IP layer is not a part of wireless communication. However, many access points are not "pure" access points and includes additional functionality such as routing and NATing.

The table below describes briefly each parameters involves the IP layer.

Setting	Description
IP Address	The IP address of the access point is not necessary for performing its basic tasks (acting as a wireless hub). The IP address is used to access the device from a web application and to facilitate the configuration process. If the access points is used as a wireless router, the IP address of the access point must be on the same subnet as the router it is attached to and proper routing rules be set up.
Netmask	See "Advanced Wireless Networking"
Gateway	IP address of the outgoing connection of your network.
DNS	IP address of the DNS server you announce by DHCP to the wireless clients

Table 1: IP related settings of an access point.

5.4 The Application Layer

The most important setting of the whole configuration process is found in the application layer, - the "admin password" of the access point. The device always comes with a default password (user: admin pass: admin) that we strongly suggest that you change immediately to a stronger password.

Avoid passwords that can be connected with you as a person or organization as they are easy to guess.
If an "unwanted" person gains access to the admin password, he/she can "hijack" your access points and change the password so that you can not reach it. In this case, the only solution is to reset the access point manually or connect via the serial interface and change password.

6. Conclusions

Configuring an access point or a wireless router can be summarized in four big steps:

- Understanding the hardware and the solution you want to build
- Setting up the wireless (physical layer) related parameters as channel, SSID, transmission power and speed.
- Setting up the wireless (link layer) related parameters as encryption or MAC access control
- Setting up the IP related parameters if you want to use the IP-functionalities of your access point as routing/NATing or DHCP server

The challenge should not be just to learn the menus of the configuration tool rather to understand what each of the parameters is doing. Every vendor will have a different configuration front-end but the "concepts" are going to be the same.