W4C

Wireless For Communities

WIRELESS Training MANUAL

10 YEARS DEF DIGITAL EMPOWERMENT foundation

Internet Society

Compiled by: Mr. Shahid Ahmad

Published by:
Digital Empowerment Foundation
House 44, Third Floor, Kalu Sarai, New Delhi – 110016, India
Tel: 91-11-26532786 / 26532787; Fax: 91-11-26532787
Email: syed.kazi@defindia.net
Web: www.defindia.net

Wireless Standard

Introduction

This chapter aims to provide brief knowledge to the reader in standards for wireless networks. We know IEEE 802.11 but what is really the technical difference between its "sub groups"?

This unit discusses not only the commonly used IEEE802.11 standards but also the new boradband standard IEEE802.16 (WiMAX).

What is the term "standard" means?

Before digging into what is the term "standard" means? wireless standards, we would like to introduce the concept of "standard" first. What is a standard by definition and why are standards important?

One aspect of standards is that technical standards of different companies are communicative between the competitors to share the market.

This is mainly due to the standardization of hardware, software and systems. For vendors, having a product that complies with a specific standard implies interoperability between products of the same family. Also a specific standard suggests the possibility to access a global market where clients that are familiar with a standard do not necessarily need to be familiar with the product itself. Standards are used by vendors to achieve a level of safety, quality, and consistency on their products. For the customer, a product that follows a specific standard implies the possibility of interoperability with other products and not to be "locked" to a single vendor.

Open and Close Standards

For simplicity, we can divide standards as Open or Close (proprietary). An Open Standard is publicly available while Proprietary standards are available under very restrictive contract terms from the organization that owns the copyright of the specification. An example for open standard is the TCP/IP specification while BlackBerry to BlackBerry Messaging standard and Microsoft Office's document format falls under close.

An open standard increases the compatibility between hardware, software or systems since the standard are available for anyone to implement. In practical terms, that means that anyone with the right knowledge can build its own product which could work together with other products following the same open standard.

An open standard may not necessarily imply that there are no licenses or patent rights. While we can assume that all free standards are open, the opposite does not necessarily need to be true. Some open standards are free of charge while for others patent holders may require a royalty fee for "using" the standard. Standards published by major international standardization bodies such as the ITU, ISO and IEEE are considered to be open but not always free of charge.

In summary, open standards are not only important for all players to create interoperable and affordable solutions but also to promote competition among vendors by setting up the clear rules of the game.

IEEE and its Working Groups

The Institute of Electrical and Electronics Engineers or IEEE (pronounced as Eye-Triple-E) is a international nonprofit organization that is the leading developer of international standards particularly in the field of telecommunications, information technology and power generation. IEEE has a set of 900 active standards and another 400 standards under development.

Some of the well known IEEE standards are the IEEE 802 LAN/MAN group of standards that includes the Ethernet standard "IEEE 802.3" and the Wireless Networking Standard "IEEE 802.11".

IEEE 802 LAN/MAN

IEEE 802 is a family of IEEE standards that refers to Local Area Network (LAN) and Metropoliton Area Network (MAN). By the definition, the IEEE 802 standards are restricted to networks that transport variable-sized packets (in contrast to cell-based networks where data are transmitted in short uniformly sized units called cells).

All services and protocols specified in IEEE 802 relates to the two lowest layers of the OSI model, the Physical Layer and the Data Link Layer.

The IEEE 802 family of standards is maintained by the IEEE 802 LAN/MAN Standards Committee. It provides an individual Working Group under IEEE 802 includes. IEE 802.11 (Wireless LAN) and IEEE 802.16 (Broadband Wireless Access) are two of those areas.

IEEE 802.11 Legacy (Wireless LAN)

IEEE 802.11 is described as the standard for "Wireless Ethernet". The original standard of IEEE 802.11 that was released in 1997 specifies Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) as the media access method, just like Ethernet does. All amendments to IEEE 802.11 are based on the same access method. However, CSMA/CA is a very inefficient access method since large amount of the bandwidth is sacrificed to ensure a reliable data transmission. This limitation is inherent to all CSMA/CA based technologies.

Furthermore, IEEE 802.11 specifies two basic data rates, 1 and 2 Mbps to be transmitted via Infrared (IR) or 2.4GHZ. Although there is no implementation based on IR, but remains as a part of the original standard.

A handful of commercial products appeared on the market using the original specification of IEEE 802.11 but was soon replaced by the IEEE 802.11b products when the "b amendment" to the original standard was ratified in 1999.

Naming confusion

IEEE 802.11 is known by many names such as Wi-Fi (Wireless-Fidelity), WLAN, and Wireless LAN and IEEE 802.11 x. Let us try to sort out this confusion regarding the name before we move on to different amendments (versions) of the IEEE 802.11 standard.

- Wi-Fi is a "brand", which is licensed by the Wi-Fi Alliance for products that meet the requirements IEEE 802.11 standard. The name "Wi-Fi" is nowadays commonly used instead of "IEEE 802.11".
- WLAN is commonly used as a name for any Wilreless Local Area Network that uses radio waves as carrier. Wire less LAN is also the alternative name of the IEEE 802.11 standard used by IEEE.
- IEEE 802.11x is sometimes used to refer to the whole group of standards within IEEE 802.11 (b, a, g etc.). The same name is also used to refer to a group of evolving standards within the IEEE 802.11 family that are under development but that have not yet been formally approved or deployed. And, the name also is often mistaken with the IEEE 802.1x standards for port-based network access control. However, there is no standard or task group named "802.11x".

IEEE 802.11 Technical Aspects

The 802.11 standard includes a set of amendments for wireless LAN. The amendments mainly differ in modulation techniques, frequency range and quality of service (QoS).

Like all standards of the IEEE 802, the IEEE 802.11 covers the first two layers of the OSI model (Open Systems Interconnection), Physical layer (L1) and Data-link layer (L2). The section below will describe what each of those layers implies in terms of wireless standards.

Layer 1 (802.11 PHY)

The physical layer has as a role to transport correctly the signal corresponding to "0" and "1" of the data that the transmitter to send to the receiver and vice-versa.

Modulation Techniques

An important parameter that influences the data transfer of certain standard is the choice of modulation technique. The more efficient the data is encoded, the higher bit rate can be achieved. On the other hand, an efficient modulation technique also requires more sophisticated hardware to handle the modulation and de-modulation of the data.

The basic and common idea behind the different modulation techniques used in IEEE 802.11 is to use more bandwidth that is theoretically needed to send one "bit" to achieve resistance against interference. The way that the information is spread leads to different modulation techniques. The most common ones are presented below. The physical layer deals mainly with data encoding and modulation.

FHSS (Frequency Hopping Spread Spectrum)

FHSS is based on the concept of transmitting on one frequency for a certain time, then randomly jumping to another. i.e. the frequency carrier changes over time or the transmitter periodically changes frequency according to a pre-established sequence. In the IEEE 802.11 standard, the defined frequency band (ISM) that spans from 2,400 to 2,4835 GHz is divided into 79 channels of 1 MHz and the jump is made every 300 to 400 ms. Hops are made around a central frequency that corresponds to one of the 14 defined channels. This modulation is not common anymore in current products.

DSSS (Direct Sequence Spread Spectrum)

DSSS (Direct Sequence Spread Spectrum) implies that for each bit of data, a sequence of bits (sometimes called pseudo-random noise, noted PN) must be transmitted. Each bit that is 1 is replaced by a sequence of bits and each bit being 0 replaced by its complement. The 802.11 physical layer standard defines a sequence of 11 bits "10110111000" to represent a "1" and its complement "01001000111" to represent a "0". In DSSS, instead of splitting a data signal into pieces and sending in different frequencies, each data bit is encoded into a longer bit string, called a chip. This modulation technique was used from 1999 till 2005.

OFDM (Orthogonal Frequency-Division Multiplexing)

ODFM, also sometimes called discrete multi-tone modulation (DMT) is a modulation technique based on the idea of frequency division multiplexing (FDM). FDM that is used both in radio and TV is based on the concept that multiple signals are sent out at the same time but on different frequencies. In OFDM, a single transmitter transmits on many (dozens to thousands) different orthogonal frequencies. Orthogonal frequencies are frequencies that are independent with respect to the relative phase relationship between the frequencies. OFDM involves the usage of advanced modulation techniques in each component which results in a signal with high resistance to interference.

An OFDM carrier signal is the sum of a number of orthogonal sub-carriers, with each sub-carrier being independently modulated commonly using some type of QAM or PSK. This is the most common modulation technique from 2005.

Frequency

802.11b and 802.11g use the 2.4 GHz ISM (Industrial, Scientific, Medical) frequency band defined by the ITU. In specific, the "L" BAND ranging from 2400 to 2483.5 MHz is used. The 802.11a standard uses 5 GHz band UNII (Unlicensed-National Information Infrastructure) covering 5.15-5.35 GHz and 5.725-5.825 Ghz.

The unlicensed 2.4 GHz band has lately become very noise in urban areas due to the high penetration of WLAN and other devices that are communicating in the same frequency range, such as microwave ovens, cordless phones and Bluetooth devices. The 5 GHz band gives the advantage of less interference but faces other problems due to its nature. High frequency radio waves are more sensitive to absorption than low frequency waves. Waves in the range of 5 GHz are especially sensitive to water and surrounding buildings or other objects due to the higher adsorption rate in this range. This means that 802.11a network is more restricted when it comes to line of sight and more access points might be needed to cover the same area as a 802.11b-based network since 802.11a. for same amount of output power, provides smaller cells than 2.4GHz.

Layer 2 (802.11 MAC)

The data link layer of 802.11 is composed of two parts:

1. Media access control (MAC)
2. Logical Link Control (LLC)

The 802.11 LLC sub-layer is identical to layer 802.2 allowing a compatibility with any other, while the MAC sublayer is redefined by standard 802.11 (L2).

MAC characterizes the access to the media in a way common to the various 802.11 standards. It is equivalent to the standard 802.3 (CSMA/CD – Ethernet) for wired networks, with functionalities specific to radio transmissions (the error rate is higher than the copper media) which are normally entrusted to the higher protocols, like fragmentation, Error Control (CRC), the retransmissions of frames and the acknowledgment of delivery.

Media Access Method

802.11b uses a protocol slightly modified compared to the CSMA/CD, called CSMA/CA (Collision Detection vs Collision Avoidance). CSMA/CA can avoid the collisions by using a basic polling method known as RTS/CTS in which the sender sends first a Request to Send (RTS) and the receiver (usually the Access Point) acknowledge the request by sending a Clear to Send (CTS) message when channel is ready to use.

During transmission between two pieces of equipment, the destination station checks the CRC of the frame and returns an ACK (acknowledgment of delivery) to the transmitter. If the transmitting station does not receive this ACK in time, it assumes that a collision occurred and the frame is retransmitted after receiving a new CTS.

The access to the media is controlled by the use of different type of inter-frame spaces (IFS), which corresponds to the intervals of time that an station needs to wait before sending data. High priority data as ACKs or RTS/CTS packets wil wait a SIFS(Shorter Inframe Space) time period than normal traffic.

While the CSMA/CA protocol permits to avoid collisions in a shared radio channel, mechanisms as RTS/CTS increases overhead (signaling frames that are necessary for the network but contain no user data) and can therefore never make the performance of 802.11b as good as CSMA/CD (collision detection) or TDMA-based technologies.

IEEE 802.11 Amendments

The most widely accepted amendments of the IEEE 802.11 family is currently b, a and g. All of them have reached the mass markets with cost efficient products. Other amendments in the family are [c-f], [h-j] and n which are enhancements and extensions or corrections to previous specifications in the family. We will take a closer look at b, a, g and n in this section.

IEEE 802.11b

IEEE 802.11b includes enhancements of the original 802.11 standard to support higher data rates (5.5 and 11 Mbit/s). IEEE 802.11b uses the same access method as defined in the original standard IEEE 802.11. IEEE 802.11b uses the DSSS modulation technique which is also defined in the original standard.

An IEEE 802.11b card can theoretically operate at 11 Mbit/s, but due to Adaptive Rate Selection scale it falls back to 5.5 and furthermore when packet loss takes place it gradually decreases up to 1 Mbit/s. Since more redundant methods are used to encode the data at lower rates, they are less sensitive to interference and attenuation (i.e. the relation of signal and noise is better at lower data rates).

IEEE 802.11a

This amendment uses the same core protocol as the original standard. IEEE 802.11a operates in the 5 GHz band and uses OFDM as modulation technique which gives it a maximum raw data rate of 54 Mbit/s. By using adaptive rate selection, the data rate is reduced to 48, 36, 24, 18, 12, 9 and, 6 Mbit/s.

802.11a has 12 non-overlapping channels whereas 8 of them are dedicated for indoor use and the remaining 4 are used for point to point links. 802.11a is NOT interoperable with 802.11b, except for equipment that specifically implements both standards.

Today, 802.11a has not reached the hype that 802.11b has. Because of restrictive regulations in the 5 GHz band in some country.

IEEE 802.11g

In June 2003, a third amendment to the 802.11 standard was ratified. It was given the name IEEE 802.11g. It also operates in the 2.4 GHz band, and uses the same modulation technique as 802.11a (OFDM) in high bit rates and can hence operate at a maximum data rate of 54 Mbit/s. To ensure interoperability with b products, at data rates of 5.5 and 11 Mbps, it reverts back to CCK+DSSS (like 802.11b) and uses DBPSK/DQPSK+DSSS for data rates of 1 and 2 Mbit/s.

It is the 802.11g interoperability with 802.11b hardware that is one of the main reasons behind its major acceptance. However, it suffers same problem as 802.11b regarding interference.

IEEE 802.11n

The latest amendment of 802.11 is IEEE 802.11n which "aims" to reach a maximum theoretical bit rate of 540 Mbit/s which would make it up to 40 times faster than 802.11b and 10 times faster than 802.11a or 802.11g. 802.11n is based on previous 802.11 amendments with greater difference, the introduction of MIMO (multiple-input multiple-output). MIMO implies that multiple transmitter and receivers are used to increase the data throughput and the transmitting range. This is considered as future technology for wireless LAN.

IEEE 802.15

Another wireless standard with a slightly different number, 802.15, is used for Wireless Personal Area Networks (WPANs). It covers a very short range and is used for Bluetooth technology.

IEEE 802.16

This protocol is used in the WiMax (worldwide interoperability of microwave accessibility). WiMax will provide high-speed broadband services and to provide mobility to the user.

Spatial Diversity

MIMO takes advantage of multi-path propagation to increase the throughput (or to reduce bit error rate) instead of trying to eliminate the effects of the unavoidable multi-path phenomena that other standards do. In simple words, MIMO takes advantage of what other standards sees as a hurdle: multi-path.

When a radio signal is sent out though the air it is spread out as a beam. The receiver receives first the main lineof- sight signal and some time later echoes and fragments of the signal that has been reflected in buildings or in other obstacles. Normally, these echoes and fragments are seen as noise to the real signal but MIMO is able to use the information of this "non direct signals" to improve the main signal. This results in clearer signals (less noise) and longer signal ranges.

Spatial Division Multiplexing (SDM)

Another feature that MIMO includes is the use of many transmitters for the same data stream, so called Spatial Division Multiplexing (SDM) where, a set of independent data streams are sent out within a single channel of bandwidth. This increases the throughput as the number of data streams is increased. Since a MIMO antenna need a dedicated processing hardware, costlythan any standard WLAN antenna.

Summary of 802.11 amendments

Below follows a short summary and comparison of the 4 most important IEEE 802.11 amendments.

Standard	Frequency	Modulation Technique	Max Data rate	Description
802.11a	5 Ghz	ODFM	54 Mbps	8 non-overlapping channels. No QoS.
802.11b	2.4 Ghz	DSSS, CCK	11 Mbps	14 overlapping channels
802.11 g	2.4 Ghz	OFDM, CCK, DSSS	54 Mbps	14 overlapping channels. Upward compatibility with the standard 802.11b
802.11n	2.4 Ghz	OFDM	360/540 Mbps	Builds upon previous 802.11 standards by adding MIMO that uses multiple transmitters and receiver antennas to allow increased data throughput through spatial multiplexing.

Table 1.1 :Summary of IEEE 802.11b/a/g/n characteristics

WiMAX (IEEE 802.16) Vs WiFi(IEEE 802.11)

WiMAX has been marketed as the future wireless technology. Many Wireless Internet Service Providers (WISPs) running solutions based on IEEE 802.11 are considering investing in WiMAX based solutions. Is WiMAX the latest "techno-hype" or does it open new opportunities for wireless broadband connectivity?

This section is reference for some of the technical differences between IEEE 802.11 and IEEE 802.16.

IEEE 802.16 has been designed specifically for Point to Multi-point outdoor environment with a single Media Access Control (MAC) that can accommodate different Physical Layers (PHY) in the frequency range of 11 to 66 Ghz. IEEE approved the initial IEEE 802.16 standard for wireless MAN in the 11-66 GHz frequency range in December 2001. The 802.16a extension for sub-11 GHz was approved in January 2003. The "802.16" standard was ratified by the IEEE in June 2004. The 802.16e standard is being reviewed by IEEE and is approved in late 2005 and officially named 802.16. The purpose of 802.16e is to add data mobility to the current standard, which is designed mainly for fixed operation.

The radio modulation technique changes depending on the frequency of operation, the packet format, medium sharing or the error control techniques are independent of the frequency of operation. The "electronics" used in the IEEE 802.16 MAC (ISO Layer 2 Data Link) are not dependent on the frequency of operation.

IEEE 802.16 does not only aim to satisfy the wireless ISP and industry requirements in almost all possible scenarios but also to become the "de facto" broadband outdoor wireless standard. It does not necessary mean that other technologies should automatically be considered obsolete.

Range and Coverage

IEEE 802.11 is a wireless LAN (indoor) protocol that was designed to operate in small cells (up to 100 meters) and in the design phase it was never considered as a Point-to-Multipoint outdoor solution. IEEE 802.11 MAC suffers from the hidden-node problem and is known for bad performance in long distance links with remote stations. The access method in IEEE 802.11 (CSMA/CA) assumes that, all nodes that are communicating with the Access Point can communicate each other to avoid collisions. Collisions in IEEE 802.11 can be avoided if all nodes can effectively sense whether the channel is occupied or not. Unfortunately, this requirement can not always be satisfied when implementing IEEE 802.11 based network in an outdoor environment. When more than ten stations are associated to the same Access Point and the rate of collisions increases, the consequent back offs and retransmissions introduce a significant waste of airtime resources. IEEE 802.11 performs bad when many users are associated to an access point in an outdoor environment. In order to solve some of these problems, proprietary solutions based on the principle of "Polling the clients" or bandwidth reservations in the IP layer has been implemented. By introducing "polling" in IEEE 802.11, the access point decides in which moment a station is granted to talk to the access point. The hidden node problem is nothing new and as soon as IEEE 802.11 was standardized there were already modifications of the IEEE 802.11 MAC to solve the problem (e.g. Karlnet TurboCell, WORP etc.). Many other proprietary solutions became available but interoperability between vendors is on testing phase. In the recent standard IEEE 802.11e the MAC was enhanced to include "polling" and make implementations interoperable.

On the contrary, IEEE 802.16 was born to be a Wireless Metropolitan Outdoor Solution. IEEE 802.16 is designed to handle distances up to 50 km. The hidden node problem was solved from the very early design phase by including DAMA-TDMA for the uplink where the base station allocates slots to each sub-station or clients. IEEE 802.16 DAMATDMA uses the same principle as a satellite network where the stations (clients) cannot hear each other.

In Non Light-of-Sight environments (NLOS), IEEE 802.16 included a more complex modulation based on 256- points of Fast Fourier Transform (FFT) of OFDM instead of the 64-points in IEEE 802.11a/g. By including 256 points instead of 64, IEEE 802.16 is equipped with a better non-line of sight capability. IEEE 802.16 can tolerate 10 times more multi path delay spread than 802.11. IEEE 802.16 can make better use of the available channel resources in an outdoor environment as the base station schedules the subscribers using dynamic scheduling algorithms. The number of subscribers does not affect the number of collisions since retransmissions of packets can occur.

In IEEE 802.16 to dedicate a certain bandwidth to a subscriber by means of TDMA, without worrying about hidden nodes, allows the introduction of smart antennas. A smart antenna combines multiple antenna elements with a signal processing capability and can optimize its beam pattern itself. IEEE 802.16 will allow advanced antenna techniques and hence better cell planning.

IEEE 802.16 has also included support for mesh networking. In mesh networking each subscriber access point is also part of the routing infrastructure. IEEE 802.16 makes a smarter “adaptive” modulation than IEEE 802.11 and enables optimization of each subscriber’s data rate by allowing the base station to set modulation schemes on a link-by-link basis. A subscriber station close to the base station can use high data rate modulation as 64QAM, while the weaker signal from a remote subscriber might only permit the use of 16QAM or QPSK.

Scalability and throughput

IEEE 802.16 has the flexibility of allocating different bandwidth in each radio channel, from very narrow channels of 1.5 MHz to a maximum of 20 MHz. The possibility of setting different channel bandwidth enables frequency reuse and better cell planning. While the number of non-overlapping channels in IEEE 802.11b is 3 and 5 in IEEE 802.11a, while in IEEE 802.16 is limited by the total available spectrum.

IEEE 802.16 allows a theoretical maximum of 70 Mbps in a 20 MHz channel. The level of actual throughput will depend on Light-of-sight, distance, air quality, interference and other factors.

Quality of Service

IEEE 802.11 includes quality of service in the new standard IEEE 802.11e (known as Wireless Multimedia or WMM). IEEE 802.11e will only support a limited prioritization on a single connection between the IEEE 802.11 access point and the station. In WMM, QoS is achieved by including shorter Interface Space (IFS) for multimedia traffic.

IEEE 802.16 has implemented QoS in a “per-flow” basis, where multiple connections between a subscriber station and a base station can have different QoS attributes. The base station polls the subscriber’s stations for bandwidth requests and schedules the traffic according to their responses.

Four types of scheduling services are supported in IEEE 802.16 depending on the type of traffic.

1. Unsolicited Grant Service (UGS), designed to support constant- bit-rate applications, such as T1 or E1 emulation and voice over IP (VoIP) without silence suppression.
2. Real-Time Polling Service (rtPS), for applications that generate periodic variable-size packets, like MPEG and VOIP with silence suppression.
3. Non-Real-Time Polling Service (nrtPS), which supports applications like FTP that generate variable-size packets on a regular basis.
4. Best Effort (BE) Service, for low-priority applications like Web surfing or e-mail.

Radio Physics

Introduction

This unit aims to provide a basic overview of radio physics and the basic principles of waves. The unit introduces electromagnetic fields and their characteristics, such as absorption, reflection, diffraction, refraction and interference, are briefly presented. The concern about free space propagation of electromagnetic waves are thoroughly discussed together with concepts as Free Space Loss, Fresnel zones, Line of Sight and Multipath.

Electromagnetic Waves:

Wave:

We are all familiar with vibration or oscillation in various forms: a pendulum, a tree swaying in the wind, and the string of a guitar. What they have in common is the periodicity, A certain number of cycles per unit of time. This kind of wave is called a ***mechanical wave,*** since it is defined by the motion of an object or its propagating medium. When such oscillations travel then we speak of waves propagating in space. For example, a singer singing creates periodic oscillations in his or her vocal cords. A stone plunging into a lake causes a disturbance, which then creates oscillations on water.

Electromagnetic waves are produced by the interaction between an electrical current and a magnetic field. Unlike other waves, the energy streams produced by the interplay of magnetic and electrical forces can travel vacuum. Just like an waves produced while playing guitar, electromagnetic streams have peaks and troughs, caused by the forces pulling and pushing at one another. An electromagnetic wave is classified according to two main criteria: ***Wavelength*** and ***Energy.*** Higher-bearing energy waves, such as gamma rays, have short wavelengths. Waves with lower energy have a much longer wavelength. The scale that describes the different types of waves is called the electromagnetic spectrum. Radio waves are typically found at the bottom of the scale,while visible light sits in the middle and the high-powered, fast oscillating gamma rays top the scale.

Wavelength: The wavelength is the distance a radio wave will travel during one cycle or can also be defined as distance between two consecutive crestend or fallend of a wave. The relation between wavelength and frequency is expressed as:

$$\lambda = c \times f$$

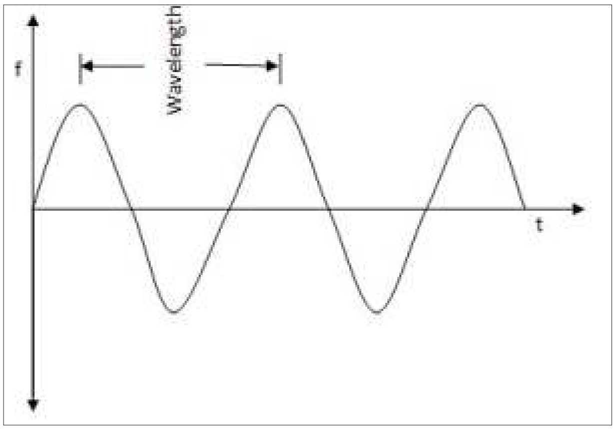


Figure 2.1: wavelength

Where λ is the wavelength, expressed in meters, c is the speed of light, which is meters/second, and f is the frequency.

Frequency	Wavelength
2.4 Ghz	0.125 m
5.0 Ghz	0.06 m

Table 2.1: wavelength for different ISM frequencies:

The speed of propagation at a certain frequency in a coaxial cable is slower than in air, so the wavelength is shorter. The velocity of propagation of electromagnetic waves in coaxial cables is usually given as a percentage of the free space velocity, and it is different for different types of coaxial cables, and is called Velocity Factor (VF).

Below follows a reminder of the denotation of the "powers of ten", which are used for all kinds of units, e.g micrometer, kilohertz, Mega Watts.

Prefix	***Quantity***		***Symbol***
Nano	10^{-9}	1/ 1,000,000,000	N
Micro	10^{-6}	1/1,000,000	µ
Milli	10^{-3}	1/1,000	M
Centi	10^{-2}	1/100	c
Kilo	10^{3}	1,000	K
Mega	10^{6}	1,000,000	M
Giga	10^{9}	1,000,000,000	G

Table 2.2 : Prefix and symbols for "powers of ten".

Amplitude and power

The amplitude of an RF signal, measured in Volts, is not of common use in the RF world. The power of a constant low frequency signal is measured in Watts, symbolized by W, and is the product of the amplitude (Volts) and the current (Amperes). One watt is also the power resulting from an energy dissipation, conversion, or storage process equivalent to one Joule per second. At high frequencies, in which energy is stored and released (as well as dissipated or converted), the relation between power, amplitude and current is more complex.

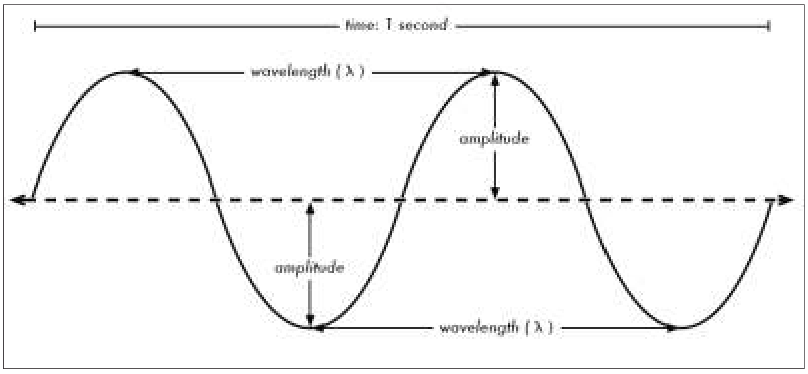


Figure 2.2: showing amplitude of wave

Wavelength, amplitude, and frequency. For this wave, the frequency is 2 cycles per second, or 2 Hz.
In a DC circuit, a source of E volts, delivering I Amperes, produces P Watts, mathematically expressed as:

$$P = EI$$

When a current of I Amperes (A) passes through a resistance of R Ohms(Ω), then the power in Watts dissipated or converted
by that component is given by:

$$P = I_2R$$

When a potential difference of E Volts appears across a component having a resistance of R Ohms, then the power in Watts dissipated or converted by that component is given by:

$$P = E_2/R$$

In a DC circuit, power is a scalar (one-dimensional) quantity. In the general RF case, the determination of power requires two dimensions, because RF power is a vector quantity. Assuming there is no reactance (opposition to RF but not to DC) in an RF circuit, the power can be determined using the above expression for DC, using root-mean-square values for the alternating current and voltage. If reactance exists, some power is alternately stored and released by the system. This is called apparent power or reactive power. The resistance dissipates power as heat or converts it to some other tangible form; this is called true power. The vector combination of reactance and resistance is known as impedance.

The electromagnetic force is carried by the photon and is responsible for atomic structure, chemical reactions, the attractive and repulsive forces associated with electrical charge and magnetism, and all other electromagnetic phenomena. Like gravity, the electromagnetic force has an infinite range and obeys the inverse-square law. The electromagnetic force is weaker than the strong nuclear force but stronger than the weak force and gravity. Some scientists believe that the electromagnetic force and the weak nuclear force are both aspects of a single force called the electroweak force.

The concept of an electromagnetic force is at the heart of the theory of electromagnetism, which explains the relationship between electricity and magnetism. Electricity and magnetism were once believed to be separate concepts, but James Clerk Maxwell changed all that back in 1873. He found magnetism and electricity to be more similar than previously thought. Magnetic poles, for example, come in pairs and attract and repel one another; electric charges have a similar duality. The relationship between electricity and magnetism can be seen when a compass is used next to an electrical source. Flipping a switch produces an electric current in the wire, which in turn produces a magnetic field that redirect the compass needle.

Physics has four "fundamental forces." The electromagnetic force is just one of them. The other three are: the strong nuclear force, the weak nuclear force, and the gravitational force. Both the gravitational force and the electromagnetic force are forces that people encounter on a day-to-day basis. The electromagnetic force plays a role in friction. It is also central to Einstein's Theory of Special Relativity.

Electromagnetiv Fields:

E and H Fields: Electromagnetic forces act between electric charges and electric currents. For every point in space, an electromagnetic field (the force felt by a charge or current at that very point) can be defined and measured.

The electric field *E* describes the force between charges and the magnetic field ***H*** describes the forces between currents.

Carrier Medium: One very important quality of electromagnetic waves is that they do not need any carrier medium unlike the mechanical wave. Examples of electromagnetic waves are light rays, X-rays, microwaves and other radio waves.

The electromagnetic field is a physical field that is produced by electrically charged objects that affects the behaviour of charged objects in the vicinity of the field. The electromagnetic field extends indefinitely throughout space and describes the electromagnetic interaction. The field can be viewed as the combination of an electric field and a magnetic field. The electric field is produced by stationary charges, and the magnetic field by moving charges (currents); these two are often described as the sources of the field. The way in which charges and currents interact with the electromagnetic field is described by Maxwell's equations and the Lorentz Force Law.

The behaviour of the electromagnetic field can be resolved into four different parts of a loop

1. The electric and magnetic fields interact only with each other
2. The electric and magnetic fields produce forces on electric charges
3. The electric charges move in space.
4. A particle at rest feels only the force due to the electric field.

Electromagnetic wave polarization: The polarization of an antenna is the polarization of the radiated electromagnetic fields produced by an antenna, evaluated in the far field. Hence, antennas are often classified as "Linearly Polarized" or a "Right Hand Circularly Polarized Antenna" or “elliptically polarized”.

A horizontally polarized antenna will not communicate with a vertically polarized antenna. Due to the reciprocity theorem, antennas transmit and receive in exactly the same manner. Hence, a vertically polarized antenna transmits and receives vertically polarized fields. Consequently, if a horizontally polarized antenna is trying to communicate with a vertically polarized antenna, there will be no reception.

In general, for two linearly polarized antennas that are rotated from each other by an angle , the power loss due to this polarization mismatch will be described by the Polarization Loss Factor (PLF):

$$\mathrm{PLF} = \cos_2 Ø$$

Hence, if both antennas have the same polarization, the angle between their radiated E-fields is zero and there is no power loss due to polarization mismatch. If one antenna is vertically polarized and the other is horizontally polarized, the angle is 90 degrees and no energy is generated.

As a side note, this explains why moving the cell phone on your head to a different angle can sometimes increase reception. Cell phone antennas are often linearly polarized, so rotating the phone can often match the polarization of the signal and thus increase reception.

Circular polarization is a desirable characteristic for many antennas. Two antennas that are both circularly polarized do not suffer signal loss due to polarization mismatch. Antennas used in GPS systems are Right Hand Circularly Polarized.

Let us take a example that a linearly polarized antenna is trying to receive a circularly polarized wave and a circularly polarized antenna is trying to receive a linearly polarized wave. What is the resulting Polarization Loss Factor?

Recall that circular polarization is two orthogonal linear polarized waves 90 degrees out of phase. Hence, a linearly polarized (LP) antenna will simply pick up the in-phase component of the circularly polarized (CP) wave. As a result, the LP antenna will have a polarization mismatch loss of 0.5 (-3dB), no matter what the angle the LP antenna is rotated to. Therefore:

$$\text{PLF (linear to circular)} = 0.5 = -3\text{dB}$$

The Polarization Loss Factor is sometimes referred to as polarization efficiency, antenna mismatch factor, or antenna receiving factor.

Classification of Polarization

The radiation field of an antenna is composed of electric and magnetic lines of force. These lines of force are always at right angles to each other. The electric field determines the direction of polarization of the wave. When a single- wire antenna is used to extract energy from a passing radio wave, maximum pickup will result when the antenna is oriented in the same direction as the electric field.

Linear Polarization: A plane electromagnetic wave is said to be linearly polarized. The transverse electric field wave is accompanied by a magnetic field wave as illustrated.

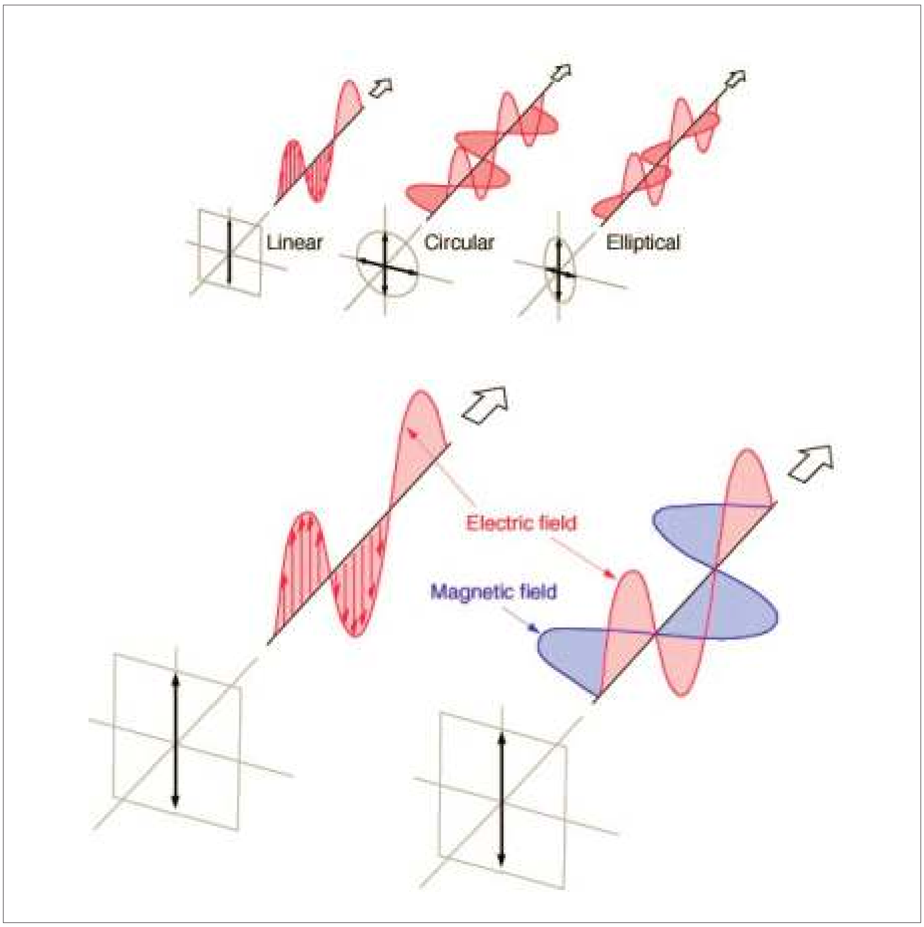


Figure 2.3: polarization of wave

Circular Polarization: Circular polarization has the electric lines of force rotating through 360 degrees with every cycle of RF energy. Circular polarization arises by two 90° phase shift income signals and also by plane polarized antennae moving 90° simultaneously. The electric field was chosen as the reference field since the intensity of the wave is usually measured in terms of the electric field intensity (volts, mili-volts, or micro-volts per meter). In some cases the orientation of the electric field does not remain constant. Instead, the field rotates as the wave travels through space. Under these conditions both horizontal and vertical components of the field exist and the wave is said to have an elliptical polarization.

Circular polarization can be right-handed or left-handed. A circularly polarized wave is reflected by a spherical raindrop in the opposite sense of the transmission. On reception, the antenna rejects waves of the opposite sense of circular polarization thereby minimizing the detection of rain. The reflection from the target will have significant components in the original polarization sense because unlike rain, aircraft are not spherical. The strength of the target signal is therefore enhanced relative to rain.

For maximum absorption of energy from the electromagnetic fields, the receiving antenna must be located in the same plane of polarization. If a wrongly polarized antenna is used, then considerable losses arise, in practice between 20 and 30 dB.

At the appearance of strong weather-clutter the controllers prefer to switch on the circular polarization. In this case the hiding effect of the targets by the weather-clutter will be decreased.

Circularly polarized light consists of two perpendicular electromagnetic plane waves of equal amplitude and 90° difference in phase. The light illustrated is right- circularly polarized.

Elliptical Polarization: Elliptically polarized signal consists of two perpendicular waves of unequal amplitude which differ in phase by 90°. The illustration shows right- elliptically polarized signal.

If the thumb of your right hand were pointing in the direction of propagation of the signal, the electric vector would be rotating in the direction of your fingers.

Dipole radiation: Dipole radiation is the electromagnetic field leaving the system of electrons swinging in a linear conductor, e.g. a straight piece of wire.This is one of the most simple forms of an antenna; the dipole antenna.

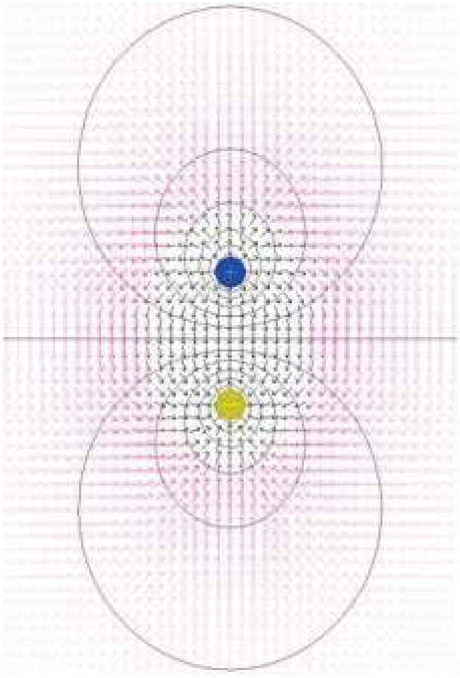


Figure 2.4: Dipole radiation

The electromagnetic spectrum

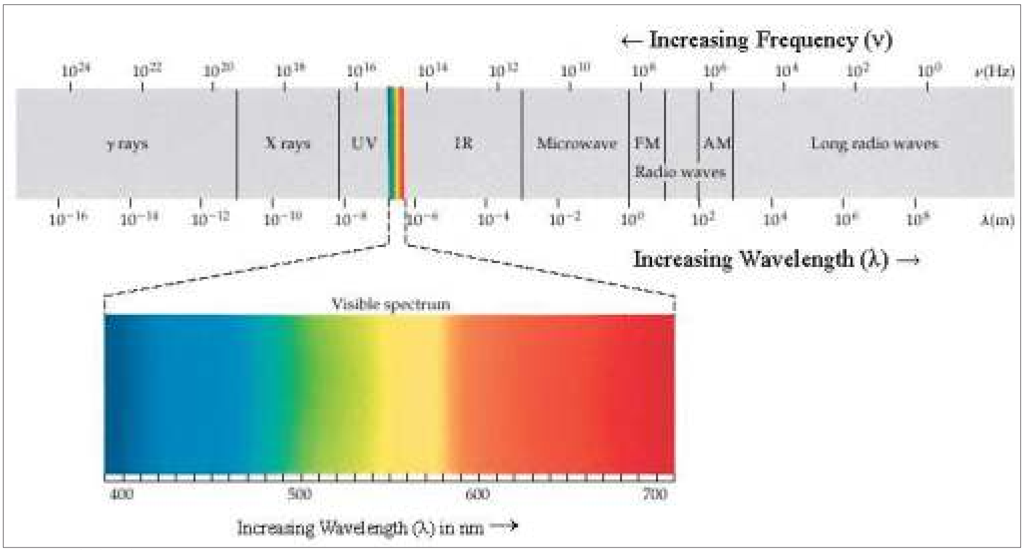


Figure 2.5 The electromagnetic spectrum

Frequencies in wireless networking

In the context of wireless networking, we predominantly focus on the ISM (industrial, scientific, and medical - license exempt) bands at

Frequency	***Standard***	***Wavelength***
2.4 Ghz	802.11 b/g	12,5 cm
5.x Ghz	802.11a	5-6 cm

Table 2.3: Frequencies and wavelengths in wireless networking

Absorption: Radio waves of whatever kind get dampened or weakened, by transferring energy to the medium they are travelling through. The power of the wave decreases exponentially in the medium, corresponding to a linear decrease in dB. Often, an absorption coefficient (in dB/m) is used to quantitatively describe the impact of the medium on radiation.

In general, we find strong absorption in conducting materials, most of all in metal. The other strong absorber for radio waves in the frequency range relevant in wireless networking (microwave range of frequencies) is water in all its forms (such as rain, fog, water pipes, and humans).

We find intermediate absorption in stones, bricks and concrete, depending on the exact parameters of the materials. The same goes for wood, trees and other material, their behavior is to a large extent determined by their water concentration. In the context of radio absorption, human beings and most animals can be seen as containers of water, thus strong absorbers.

Reflection: We are all familiar with the reflection of visible light in mirrors or on water surfaces. For radio frequencies, reflection mainly occur on metal, but again also on water surfaces and other suitable materials. The basic principle of reflection is that the wave is reflected back in the same angle it hits a surface.

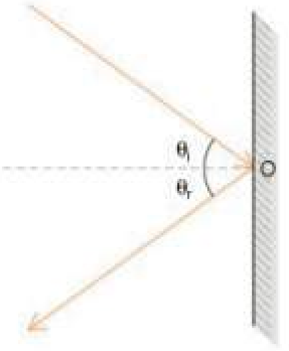


Figure 2.6: Reflection of a wave, same outgoing angle and the incoming angle.

Two important cases of reflection are reflection on a plane surface and reflection of a parabolic surface.

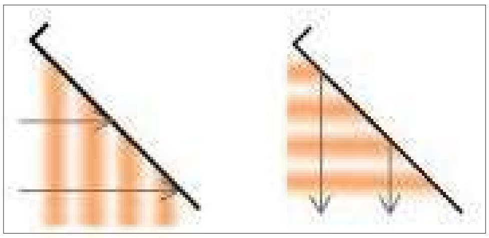


Figure: 2.7: Reflection on plane

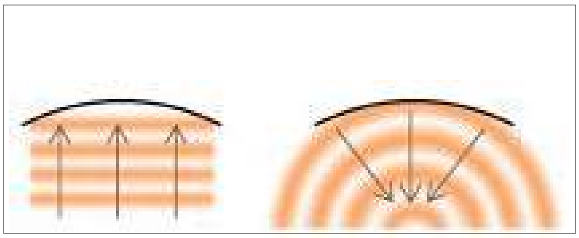


Figure2.8: Reflection on parabola

Diffraction: Diffraction is a phenomenon that is based on the fact that waves do not propagate in a single direction. It occurs when waves are propagating though a medium and diverge into wider beams. Diffraction implies that waves can be "bent" around corners.

Diffraction is a direct consequence of the Huygens principle, and it scales roughly with the wavelength. This means that we can expect waves to bend more easily the bigger is the wavelength. That is the reason why an AM Radio station operating at 100 kHz can be heard easily (the wavelength is 3 kms) while in wireless communication line of sight between sender and receiver is required (the wavelength is 12 cms)

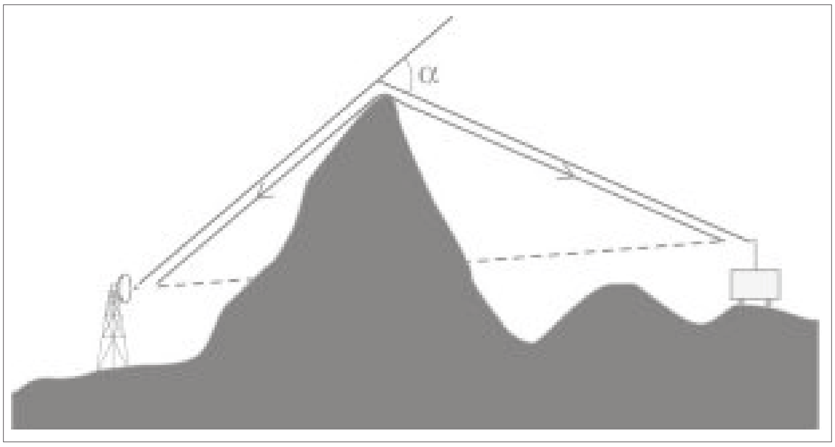


Figure 2.9: Showing diffraction of electromagnetic wave

Refraction: Refraction is the apparent "bending" of waves when they meet an obstacle with a different density. When a wave moves from one medium to another of a different density, it changes speed and direction when entering the new medium.

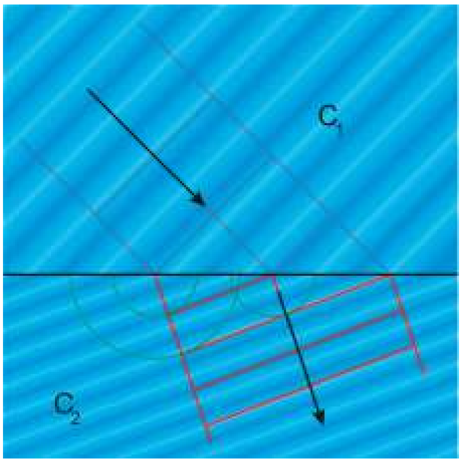


Figure2.10: Wave refraction

The lines in C1 represent the incoming waves while the lines in C2 represents the by refraction "bended" waves. C1 is a medium with less density than C2. The angle that the waves break into depends on the density of the material of the obstacle (C2)

Interference: Waves of the same frequency and a fixed phase relation (relative position of waves) can annihilate each other, so that one wave plus another wave equals zero.

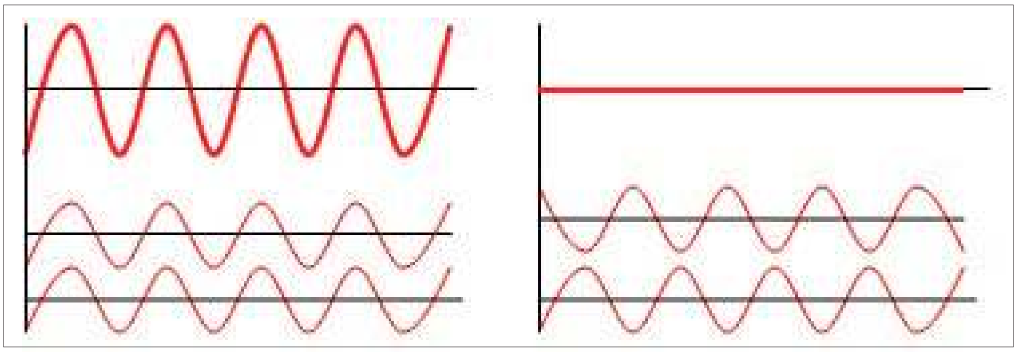


Figure 2.11: Showing maximum amplification and Complete annihilation

For this to occur in its purest form (complete annihilation or maximum amplification), waves would have to have the exact same wavelength and energy and a fixed phase relation. In wireless technology, the word interference is typically used in a wider sense, for disturbance through other RF sources, e.g. neighboring channels.

Effects dependence of frequency

Effects are more or less present depends on the frequency of the wave. Mathematical expressions to calculate these effects are complex in nature, however, a few very simple rules of thumb prove to be very handy in understanding and planning radio propagation.

1. The lower frequency, the further it goes
2. The lower frequency, the better it goes through and around things
3. The higher frequency, the more data can transport

Radio propagation in free space

In the following section we will take a closer look at four relevant effects and concepts in radio propagation.

- Free Space Loss (FSL): the fact that a radio wave loses power even along a straight line through a vacuum
- Fresnel Zones: the fact that radio waves travel through a wide cigar shaped zone rather than just on a straight line
- Line of Sight: LOS is considered if there is a clearance of 60% in the first Fresnel zone.
- Multipath Effects – the fact that one initial signal might find different ways to reach a given receiver

Free space loss (FSL)

The majority of the power of a radio signal will be lost on free space. The Free Space Loss measures the power loss in a free space without any kind of obstacles. The radio signal weakens while expanding into a spherical surface.

The power loss of electromagnetic waves in free space is proportional to the square of the distance and also proportional to the square of the radio frequency. In the relative unit decibel (dB), that results in:

$$FSL(dB) = 20\log_{10}(d)+20\log_{10}(f)+K$$

d = distance
f = frequency
K = constant that depends on the units used for d and f
If d is measured in meters, f in Hz and the link uses isotropic antennas, the formula is:

$$FSL(dB) = 20\log_{10}(d)+20\log_{10}(f)-147.5$$

As a rule of the thumb in a 2.4 GHz wireless network, there is a loss of 100 dB for first kilometer and loss increases by 6 dB every time as the distance doubles. A 2 Kms link has a loss of 106 dB. While a 4 Kms link has a loss of 112 dB.

Fresnel zones: Remembering the Huygens principle, it is easy to see that also the points that are not in the direct axis between A and B radiates some power towards the receiving point B. A detailed analysis taking into account interference between all the different waves is beyond the scope of this unit, however its result is essential for us to arrive at a conclusion. The expression resulting from above analysis for the first Fresnel zone, which should be kept free in order to transmit a great part of the power from A to B.

If there are obstacles inside of the Fresnel zone, the reflections of the waves in those obstacles can provoke higher attenuations of the signal in the receiving point B.

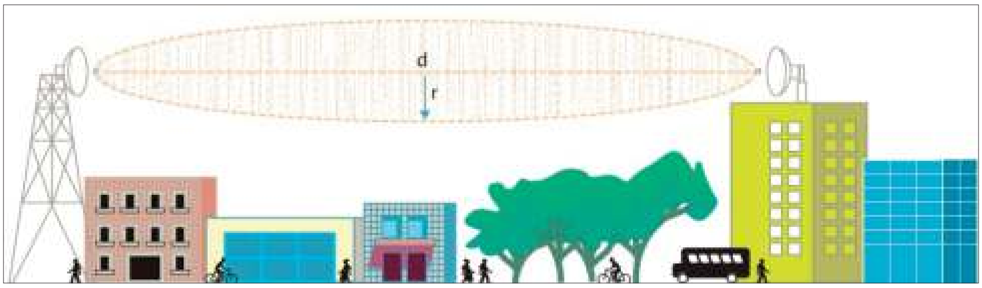


Figure 2.12: Fresnel Zone

The formula for the first Fresnel zone is:
r= 17.32√(d/4f)
d = distance [km]
f= frequency [GHz]
r= radius [m]

A radio link of 9.6 Kms will require that there are no obstacles of path in r=17.32 meters under the direct line of sight.

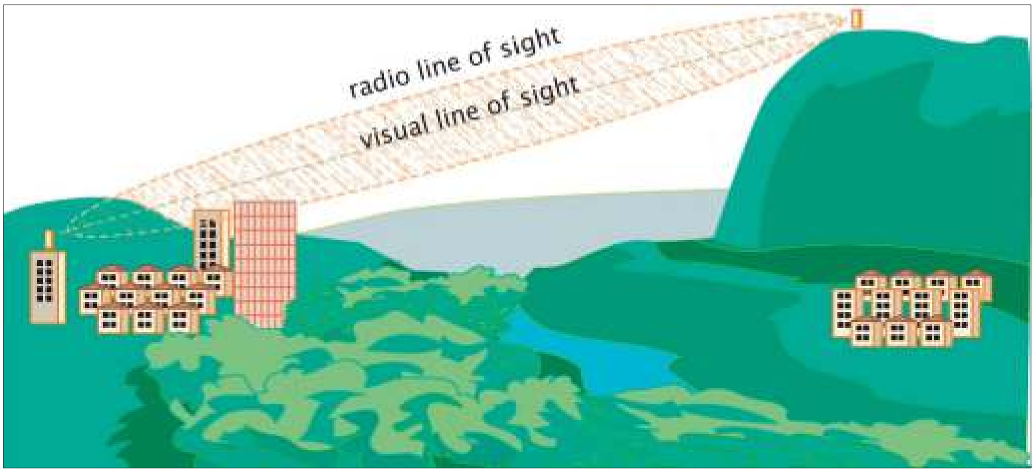


Figure2.13: showing Freshnel zone

Line of sight: For visible light, the line of sight is easy to understand and verify. However, things are a bit more complicated for radio links as they are not visible for our eyes. In general, we need to have a free (optical) line of sight (LOS) for a radio link. Additionally, we need "a bit of space around it", as defined by the Fresnel Zones.

Line of sight (LOS) vs visual line of sight.

Multipath: A radio wave can reach the receiving side via many different paths by reflection. Delays, interference and partial modification of signals can cause problems when receiving the signal.

However, the effects of multipath are not all bad signals level and we can sometimes take advantage of multipath effects in order to overcome the limits of line of sight. A non-line-of-sight (NLOS) link can become possible with wireless technologies that are robust enough against multipath effects to let them contribute to the transmission of signals..

Radio Link

Introduction

Good wireless equipment we have and how clear the Line of Sight is, we need to calculate your Link Budget. Overpowering a radio link will not necessary make things better for your implementation and your neighbours.

Having a good link budget is essential as it is the basic requirement of a functioning link. It can be compared with the foundation of a building. For example it does not matter how well the floors, walls and roofs are built if the foundation is weak, the whole building will collapse on time.

What is a Link Budget?

A wireless link budget for a Point to Point radio link is the accounting of all of the gains and losses from the radio transmitter (source of the radio signal), through cables, connectors and free air to the receiver. Estimating the value of "power" in different parts of the radio link is necessary to be able to make the best design and the most adequate choice of radio equipment.

The elements of a link budget

The elements can be broken down into 3 main parts:

- Transmitting side with effective transmit power
- Propagation part with propagation losses
- Receiving side with effective receiving sensibility

A complete radio link budget is simply the sum of all contributions (in decibels) across the three main parts of a transmission path. All positive values are gain and all negative values are losses.

$$T_P - CL_{TX} + G_{TX} - FSL + G_{RX} - CL_{RX} = \text{Margin} - R_S$$

Tp → Transmitter power [dBm]
CLTX → Cable loss in transmitter side [dB]
GTx → Antenna gain Transmitter side [dBi]
FSL → Free Space Path Loss [dB]
GRx → Antenna gain receiver side[dBi]
CLRx → Cable RX loss [dB]
Rs → Receiver Sensitivity [dBm]

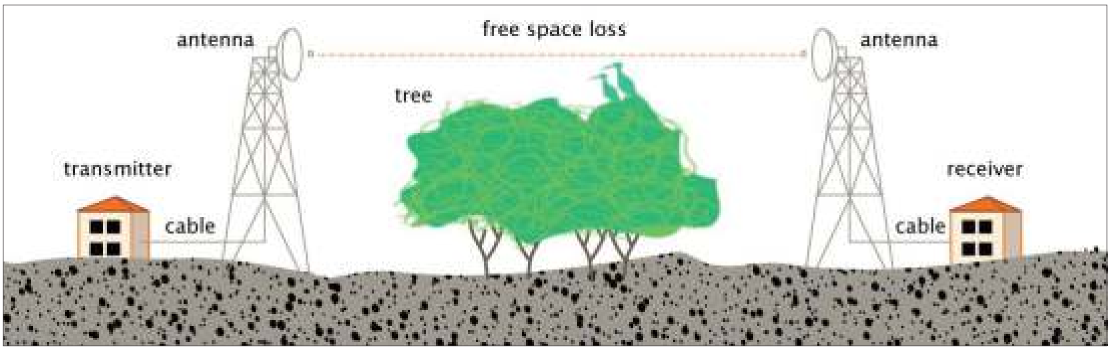


Figure 3.1: The full transmission path from transmitter to the receiver.

Transmitting side

Transmit power (Tx): The transmit power is the power output of the radio card. The upper limit depends on regulatory limits on country/region and point in time. The transmit power of your card can normally be found in the vendor's technical specification. Keep in mind that while the technical specifications will give we lab values, real life values may vary with factors like temperature and voltage.

Typical transmission power in IEEE 802.11b equipment ranges from 15 - 20 dBm (30-100 mW).

Protocol	*Peak power [dBm]*	*Peak power [mW]*
IEEE 802.11b	18	65
IEEE 802.11a	20	100

Table 3.1: power used in IEEE 802.11 protocol

Cable Loss: Losses in the radio signal will take place in the cables that connect the transmitter and the receiver to the antennas. The losses depend on the type of cable and frequency of operation and are normally measured in dB/m or dB/foot. Typical loss in cables is 0.1 dB/m - 1 dB/m. Consider that we are using a RG58/BNC cable, which has a loss of 1dB/m, to connect a transmitter to an antenna. Using 3 meters of RG58 cable is enough to lose 50% of the power (3dB).Cable losses are very much dependent on frequency. So when calculating the loss of your cable, make sure we use the right values for your frequency range used. Check the distributor's data sheets and if possible, verify the losses taking your own measurements. As a rule of thumb, we can count with double amount of cable loss [dB] for 5.8 Ghz compared with 2.4 Ghz

Cable type	*Loss [db/100m]*
RG 58	ca 80-100
RG 213	ca 50
LMR-200	50
LMR-400	22
Aircom plus	22
LMR-600	12
½” Flexline	14
7/8” Flexline	6,6
C2FCP	21
Heliax ½ “	12
Heliax 7/8”	7

Table 3.2: Typical values of cable loss for 2.4 Ghz..

Loss in connectors: Typically 0.25 dB (loss) for each connector is considered as less on connector. This value applies for properly made connectors while badly soldered DIY connectors will imply higher loss. Check data sheets for losses at your frequency range versus available connector type.

If long cables are used, the accounting of the connector losses is normally included in the “cable loss” part of the quation. But to be on the safe side, always assume an average of 0.3 to 0.5 dB loss per connector as a rule of thumb. Additionally, lightning arrestors that typically are used between antennas and the radio gear behind them should be budgeted for 1 dB loss.

Amplifiers: Amplifiers can be used to compensate for cable loss or for signal boosting. In general, the use of amplifiers should be seen as a last option. Intelligently optimized antennas and high sensitivity in the receiver are better than brute force amplification.

Quality amplifiers depends on frequency characteristics (broadening) and add extra noise to the signal. We must consider the legal limits of the region while adding amplifiers.

Antenna Gain: A typical antenna gain ranges from 2 dBi (simple integrated antenna) to 5 dBi (standard omni directional) up to 25-30 dBi (parabolic).

Propagation Losses

The propagation losses are related to all attenuation of the signal that takes place when the signal has left the transmitting antenna until it reaches the receiving

Free Space Loss: The majority of the power of a radio signal will be lost in the air. Even in vacuum, a radio wave loses some of its energy since (according to the Huygens Principle) some energy is always radiated in directions other than our link axis. Note that this has nothing to do with air, fog, rain or any other influence that will further add losses.

The Free Space Loss (FSL) measures the power loss in free space without any kind of obstacles. The radio signal weakens in free space due to expansion into a spherical surface. FSL is proportional to the square of the distance and also proportional to the square of the radio frequency. In decibel, that results in the following equation:

$$FSL(dB) = 20\log_{10}(d)+20\log_{10}(f)+K$$

d → distance
f → frequency
K → constant that depends on the units used for d and f
If d is measured in meters, f in Hz and the link uses isotropic antennas, the formula is:

$$FSL(dB) = 20\log_{10}(d)+20\log_{10}(f)-147.5$$

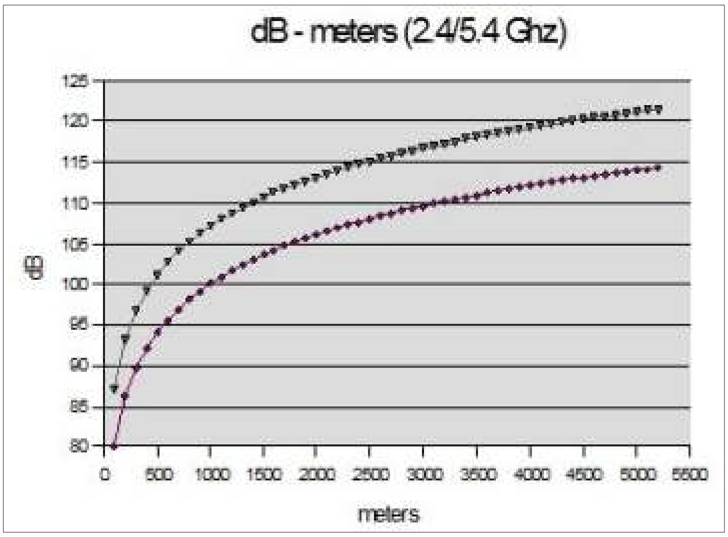


Figure3.2: dB Linear approximation after 1.5 Km

The Figure3.2 shows the loose in dB for 2.4 GHz and 5.4 GHz. We can see that after the 1.5 km, the loose can be seen as "lineal" in dB.

As a rule of thumb in a 2.4 GHz wireless network, 100 dB are lost in the first kilometre and the signal is reduced by 6 dB every time that the distance doubles. That implies that a 2 km link has a loss of 106 dB and a 4 km link has a loss of 112 dB and goes on.

Distance [km]	***915 MHZ***	***2.4 Ghz***	***5.8GHz***
1	92 dB	100 dB	108 dB
10	112 dB	120 dB	128 dB
100	132 dB	140 dB	148 dB

Table 3.3: Free Space Loss (FSL) in dB for a set of distances and frequencies.

These values are theoretical values and can very well differ from your measurements. The term "free space" is never quite so "free", and the losses can many times be larger due to terrain influences and climatic conditions.

Fresnel zones: We can calculate the zones, the space around an axis that relevantly contributes to the transfer of power from source to destination.

Based on this, we can then find out what the minimum distance of an clearance from our axis should be.

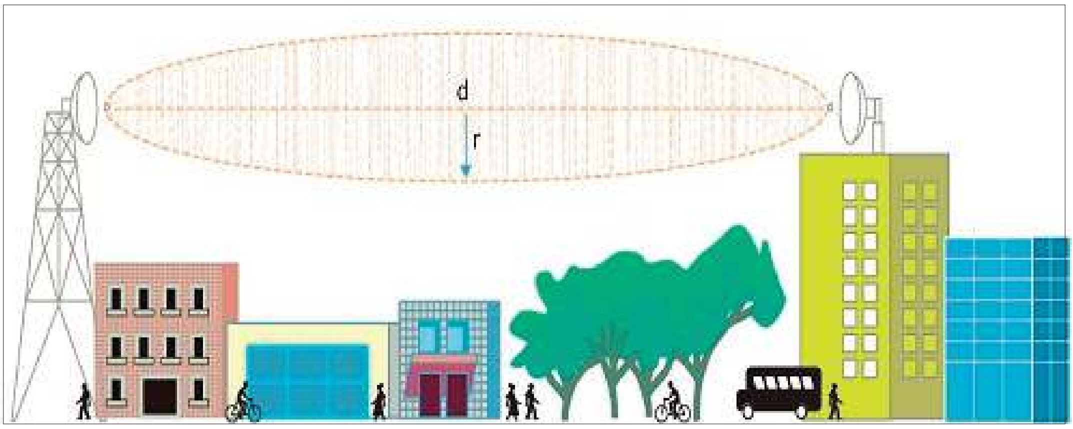


Figure 3.3: Fresnel zones

Most wireless professionals work with an approach that demands that the first Fresnel zone be unobstructed, although one might be more demanding. Others demand a radius containing 60% of the total power unobstructed.

The formula below calculates the first Fresnel zone.

$$r = 17.13\sqrt{(df/4f)}$$

Where d is distance between the transmitter and receiver

To calculate radius of first Fresnel zone from transmitter to fixed obstacle of distance d1 from the transmitter and d2 from receiver then

$$r = 17.31\sqrt{((d_1 \times d_2)/(f \times d))}$$

d1= distance to obstacle from transmitte
d2 = distance to obstacle from receiver
d = distance [km]
f= frequency [GHz]
r= radius [m]

Distance[km]	*915 MHZ*	*2,4 Ghz*	*5,8 Ghz*	*Height [m] (rel. earth*)*
1	9	6	4	0,02
10	29	18	11	2
100	90	56	36	200

Table3.4: Radius [m] for the first Fresnel zone

Receiver side: The calculations are almost identical to the ones at the transmitter side.
Antenna Gain on receiver side: See Antenna Gain on transmitter side.
Amplifiers on receiver side: The calculation and the principles are the same as on the transmitting side. Amplification is not a recommended

Receiver sensitivity: The sensitivity of a receiver is a parameter that deserves special attention as it indicates the minimum value of power that is needed to successfully decode/extract "logical bits" and achieve a certain bit rate.

The lower the sensitivity, the better is radio receiver. A theoritical value is -82 dBm for a 11 Mbps link and -94 dBm for a 1 Mbps link.

A 10 dB difference here (which easily can be found between different cards) is just as important as a 10 dB gain that might be won by the use of amplifiers or bigger antennas.

Card	*11 Mbps*	*5,5 Mbps*	*2 Mbps*	*1 Mbps*
Orinoco cards PCMCIA Silver/Gold	-82 dBm	-87 dBm	-91 dBm	-94 dBm
Senao 802.11b card	-89	-91	-93	-95

Table 3.5: Typical values of receive sensitivity of wireless network cards.

Margin and SNR: Although the signal received in the receiver is bigger than the sensitivity, it is required to be in certain margin between noise and signal to achieve a certain data bit rate.

The relationship between noise and signal is measured by the signal to noise ratio or SNR. A typical requirement of SNR is 16 dB for a 11 Mbps connection and 4 dB for the lower speed of 1 Mbps.

In situations where there is very little noise, the radio link is first limited by the sensitivity of the receiver. In urban areas where there are many radio links operating, it is common to see high levels of noise (as -92 dBm). In those scenarios, the radio link is limited by the need of a high received signal to satisfy the Signal to Noise (SNR) condition.

$$\text{Signal to Noise Ratio[dB]} = \text{Log10(Signal Power[W]/Noise Power[W])}$$

In normal conditions without any other source in the 2.4 GHz band and without industrial noise, the noise level is around -100 dBm.

Terms and Concepts: There are a number of terms and concepts we will meet when dealing with radio link calculations.
Link Budget / Power Budget / System Gain: All of these concepts basically mean the same thing: a calculation of signal/power throughout the system.

System operating margin: This value tells us the difference between the signal value and the sensibility.

EIRP (Effective Isotropic Radiated Power) The Effective Isotropically-Radiated Power (EIRP) or the Maximum Radiated Power is regulated by the national radio regulatory authority. It specifies the maximum power that is legally permitted to be sent out to the free air in a specific country/area. The legal limit in Europe is normally 100 mW. In some very concrete scenarios (point-to-point links) and in some countries outside of Europe, the maximum allowed radiated power is 1 - 4 W.

EIRP is a measure of the effective output of a system and is expressed as equivalent to an isotropically radiating system. In simple words, this parameter tells we how strong we are allowed to send your signal in the air.

The Radiated Power is the result of subtracting power losses in the cable and connectors to the Transmitter Power and adding the relative "gain" of the antenna.

Radiated Power (dBm)
= Transmitter Power (dBm) – Losses from cable and connectors (dB)
+ Antenna Gain (dBi).

Calculating with decibel (dB, dBm, dBi)

Dimensionless Unit

A link budget is the accounting of all of the gains and losses from the radio transmitter (source of the radio signal), through cables, connectors and free air to the receiver.

Transmitter power [dBm] – Cable TX loss [dB] + Antenna TX gain [dBi] -
Free Space Path Loss [dB] + Antenna RX gain [dBi] – Cable RX loss [dB]
= Margin – Receiver Sensitivity [dBm]

One aspect that might be surprising is that the equation is adding dBm, dB and dBi units like they were of the same dimension. How is it possible to simply add and subtract dBm, dB and dBi?

The answer lies in the face that the decibel (dB) is a measure of the "ratio" between two quantities and it is a dimensionless unit like percent (%). Hence, different "kinds" of decibel units can be added and subtracted and the results will remain dimensionless.

Converting Watt to Decibel

To be familiar with conversion between power (W) and decibel comes very handy when dealing with link calculations.
In link calculations, tree different types of decibel occur.
dB (decibel)
Used for measuring losses in cables and connectors. Decibel is the relative unit compared to 1 W.

dB = 10 * log(P(W)/1W))

dBm (decibel milli)
Transmitted power is normally expressed in (dBm). A dBm is a decibel relative unit compared to 1 milliwatt (0.001 W).
The conversion between power (W) and dBm is calculated as following:

dBm= 10 * log(P/0.001) = 10*log(P(W)/1Mw))

dBi (decibel isotropic)
Used for expressing the antenna gain..

dBi = dB relative to an ideal isotropic antenna

When using dB as a way to calculate the power the following "guidelines" are useful to remember:
Duplicating the power is equal to adding 3 dB
Reducing the power by half is equal to subtracting 3 dB

Let us say that we have a transmitting power of 100 mW (20 dBm).
If we duplicate the power of the transmitter to 200 mW, we add 3 dB to 20 dBm which gives us 23 dBm.
In that way, 400 mW gives us 26 dBm and 800 mW gives us 29dBm.
Following the same reasoning implies that 50 mW is 17 dBm (20 dBm - 3 dB).

Complete Link Budgets

Calculating link budgets is all about making sure that the margin in the receiver side is higher than a certain threshold. Furthermore, the EIRP must be within regulations.

The margin of a link budget can be summarized as follows:

$$\begin{aligned}\text{Margin} = {} & \text{Transmitter power [dBm]} - \text{Cable TX loss [dB]} \\ & + \text{Antenna Tx gain [dBi]} - \text{Cable TX loss [dB]} \\ & + \text{Antenna RX gain [dBi]} - \text{Cable RX loss [dB]} \\ & - \text{Receiver Sensitivity [dBm]}\end{aligned}$$

The following section will provide two realistic examples of link budgets, one for a 50 km link and another for a 1 km link.

Example 1: 50 km Link

Distance: 50 kms (31,1 miles)
Frequency: 2,4 Ghz

Element	***Value***
Transmit Output	+ 15 dBm
Cable and Connectors	- 3 dB
Antenna TX	+ 24 dBi
FSL	-134 dB
Antenna RX	+ 24 dBi
Cable and Connectors	- 3 dB
Receive Sensibility	- 85 dBm
Total: (margin)	+ 8 dB

Table3.6: path loss calculation in 50Km link

The margin of this link is 8 dB and the transmitting power is 36 dB (> 3 W). This link might not be legal on some country/region.

Example 2: 1 km Link
Distance: 1 km (0,622 miles)
Frequency: 2,4 GHz
Low quality cabling
Low antenna gain

Element	***Value***
Transmit Output	+ 18 dBm
Cable and Connectors	- 5 dB
Antenna TX	+ 5 dBi
FSL	-100 dB
Antenna RX	+ 8 dBi
Cable and Connectors	- 5 dB
Receive Sensibility	- 92 dBm
Total: (margin)	+ 13 dB

Table 3.7: path loss calculation in 50Km link

The margin of this link is 13 dB and the transmitting power is 15 dB (< 50 W). This link is legal.

Other relevant calculations and approaches

In addition to the elements considered so far, we have to take into account correction factors due to terrain and building structures, climatic factors, and many others. All of these are very empirical by nature.

We will find them under terms like rain fade, urban fade, terrain fade, with a lot of different approaches to calculate them properly. However, there are limits to these theories as the factors that can NOT be easily calculated or predicted, are normally the ones that decide whether a link works or not. In a long distance link, factors like rain, fog and even a changing in vegetation conditions can easily contribute loss up to 15 dB.

Antenna tilt

Antenna tilt to compensate for earth curvature and tower height differences:

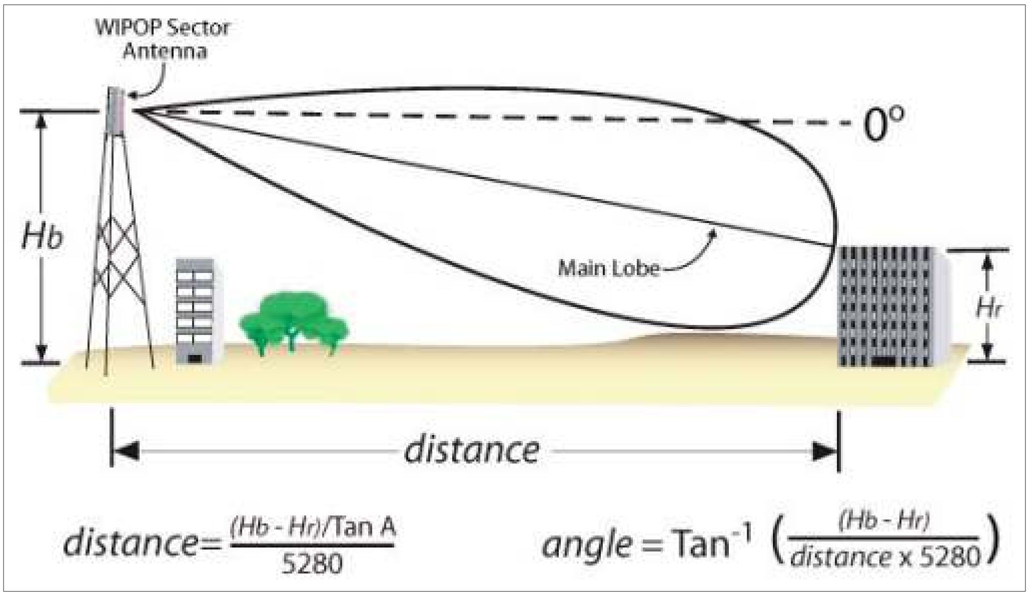

WIPOP Sector Antenna
0°
Hb
Main Lobe
Hr
distance
distance= (Hb - Hr)/Tan A / 5280
angle = Tan-1 ((Hb - Hr) / distance x 5280)

Figure 3.4: showing antenna tilt

Notes:

- Horizon means that the -3dB point on the main lobe shoots off into the horizon and does not touch the earth (assuming flat terrain.)
- The formula for calculating the distance is ((Hb - Hr) / Tan A) / 5280 where A is the angle
- The formula for calculating the angle is Tan-1 * ((Hb - Hr)/ (D * 5280))
  where D is the distance

Bearing Angle

The bearing angle (towards true north) and the distance from latitude/longitude can be calculated as:

distance = r * arccos[sin(lat1/57.2958) * sin (lat2/57.2958)
+ cos(lat1/57.2958 * cos (lat2/57.2958) * cos(lon2/57.2958 – lon1/57.2958)]

lat, lon in metric degrees

We have discussed about link calculation but this is important for implementation of a wireless (link) network in terms of project planning and budgeting of equipment.

A detailed implementation plan of a wireless network is necessary to be able to produce a good and consistent budget. A good implementation plan should not just consider the physical location of the wireless equipment or our chosen technology and vendor but also which extra resources are needed to get a link up and running.

Sustainability aspects need also to be included in the implementation plan. The budget should also consider backup resources when things "go wrong!!!" In this discussion we show how being able to make a good implementation plan allows us to produce a good budget in terms of equipment and logistics. The final cost of the wireless project can easily go well above your initial budget if other aspects (not wireless related) are not considered in your planning. When we build wireless networks, we must consider non-wireless elements too. It is not about buying the most expensive technology; it is about having a good plan how to use those radios or link.

Viability study

The project should start with a detailed *viability study.*

Make sure that the consultant (commonly known as "expert") that we hire is going to be able to answer all your questions and justify properly his recommendations. An external and independent person that can review the results of the "expert" is also recommended.

Make sure that the viability study is always presented to we or your organization face-to-face. It is a good idea that we have at least one week to go through the written report in advance.

Request/consider that the viability study answers the following four questions.

- What physical infrastructure is available on site?
- What technical infrastructure is already in use at the site?
- Where is the closest point of presence for power/energy at site?
- Where is the closest point of presence for Internet connection or communication on site?

These four questions have great impact on the final price tag of the wireless implementation. Each and one of them will carefully be discusses below.

Additional facts that are of importance for the pre-study are:

- Weather conditions on site (temperature, amount of rain, thunder, humidity)
- Type of terrain (sand, soil, stones)
- Population (sparsely or dense populated)
- Access to road for transportation
- Radio/tower Legislation
- Conditions for importing equipment
- Communication factors

Site survey of existing physical infrastructure

In order to be able to evaluate your options for the exact location of the implementation, start by studying existing suitable physical infrastructure on site in terms of existing masts, towers or high buildings. Ask for available and updated maps of the area to make a theoretical study before making the on-site visit.

The more information we possess in advance, the better chances we will do something useful when we move to the site.

If masts or towers already exist, there might be a chance of co-location sharing with other operators rather that building your own tower. If the site is located in a densely populated area, the regulators might not allow we to establish a new tower, due to certain regulations in populated areas.

The most practical solution is always to use an existing roof top that suits your implementation. Working at the top of a building implies easier maintenance of equipment and no need of maintaining big masts or towers. If neither a tower nor a roof top is available on site, we must consider building the necessary infrastructure yourself.

The site survey is a very important "social engineering" task, we need to identify the *key people* that can help we establish your infrastructure. Do not forget to keep records of all names of people that we talked to during your site survey research.

During the on-site visit there are a number of things that should be noted:

- If many possible sites exist, perform a survey on those places by making relevant measurements with portable WLAN equipment running Netstumbler (Win32), Wavemon (Linux) or similar software for 2.4 GHz frequency band.
- The distance to the other point(s) must be measured so that a proper link budget can be performed before we start to order and purchase equipment.

The distance can be measured either with GPS equipment (preferable) or with an updated and accurate map with scale. If neither of that is available, the distance can be measured manually by car or a bike equipped with a "trip meter".

- Bring binoculars to perform a line-of-sight test to the other endpoint and a digital camera for documentation of the site.
- Use blinking lamp or torch to communicate with the other node.
- Bring tape measure, long light rope, climbing gear (including helmet).
- When measuring distances try to image the path that the cables are going to take to obtain accurate figures.
- Be pessimistic! It is better to have 5 extra meters of cable that miss one extra meter at the top of a 40 meters hight tower.
- Nearest power source or electric source and tis voltage level.

Site survey of existing technical infrastructure

If any kind of technical infrastructure exists on the site where we want to implement the link, start by contacting your new neighbors to get the necessary information regarding their equipment so that we can plan your project without interference. Also, discuss possibilities for co-location with them.

Other information that we should obtain are:

- Existing wireless infrastructure
- Existing antennas and cabling
- IP Network address (if we are going to share IP infrastructure)
- Description of other equipment on site (take pictures of all specifications/labels)
- Frequencies/Channels.
- Radio power
- Voltage or power backup
- Techincal person

Access to power/energy

Access to electricity on the site is of course vital. To ensure reliability of your service the source of electricity also needs to be reliable. In countries with frequent power cuts and frequency fluctuations, a UPS is mandatory.

If the equipment is goiing to be placed on a roof top, powering the equipment with electricity might not be so complicated. But, if your tower needs to be far away from the closest power grid, we might have to work a bit harder.

If the distance to the closest power grid is reasonable, we should ask the power company for permission to hook on to the network by digging down an extension cable to the grid. Most probably, the connection to the grid has to be performed by the power company themselves.

If the distance is too long or digging is not feasible for other reasons, we should consider another source of energy as wind or solar panels. When we budget for energy we should not only budget for the equipment (solar panels, batteries, wind mild, diesel group) but for a fix cost of installation, transport and yearly maintenance cost.

Note about cables: When dealing with cables (data or electricity) think of a proper installation. Think of rats, sun, ice, wind and thieves.

Communication factors

In most of the cases we will need to procure a source of Internet access at the exact location where the wireless equipment will be located. That implies that we must extend the Internet connection from one place to the physical location of your wireless equipment.

Avoid, if possible, using another wireless link to the top of a tower or roofing (your wireless backbone). Having an additional wireless link can have serious implications in the overall performance of the main wireless backbone link.

Either reserve one single frequency/channel to link the Internet to your backbone or Wire the Internet connectivity to your wireless backbone.

When bringing the Internet to your wireless network try to avoid any possible traffic bottlenecks.

Whether the cable is dug down or placed over ground, the cable needs to be protected from its surroundings in terms of weather and animals. The first enemy of cables are rats and without a proper PVC protection the cable will soon be damaged. PVC pipes can be dug down or left on the ground. When procuring PVS pipes, make sure that we purchase one that suits your implementation since there are many different PVC pipes on the market depending on climate, depth and other parameters. The PCV pipes must also be properly connected to each other (with glue) so that the whole construction is watertight..

- Always aim for a fibre or copper connection between the uplink and the backbone since a wireless link will affect the overall performance negative.
- Protect the fibre/copper with PCV pipes or similar to its extended lifetime.
- Think of external environment(like temperature, animal, thieves)

Budgeting Issues

A hardware budget for a wireless implementation requires a lot of thinking. Except for the actual cost of radio and network equipment, there are a set of other items that we should consider. This section points out a few things that should not be forgotten when doing a hardware budget.

Electricity

In many developing countries, the demand for electricity is more what the provider can deliver. The situation in many countries is not stable enough to directly plug electronic equipment into grid powered outlets as the power may be fluctuating, which damages electrical equipment. The solution to the unstable power is to add batteries, battery chargers, AVR(automatic voltage regulator), and inverters to those node in the system. These backup systems are relatively inexpensive and are very effective at providing both surge protection and a consistent power supply.

The chargers are connected to the electricity grid and keep the batteries charged whenever power is available. Inverters continually supply 240V/110V AC to the devices from energy stored in the batteries. In this way, anything plugged into the system is never fed with power straight from the unstable voltage. The only part of the system vulnerable to damage from power surges is the charger, which may be cheapest part of the system and easier to replace than radio equipment.

There are off the shelf uninterruptible power supplies (UPS) that use similar systems, called an online UPS. These are different from the standard UPS because power is always going through filters and rectifiers. A standard UPS uses line interrupt technology, the electricity from grid to equipments. The problem with this is surge voltage may pass to equipments. An online UPS converts the grid alternating current (AC) to direct current (DC), and then rectifies it back to AC. Power in the output plugs of the UPS is never direct from the power grid and it always takes surge voltage from batteries then provides to equipments.

These things should be taken into consideration when choosing the for an implementation.

Electrical grounding and Lightening protection

An installation located on any plaace needs protection against lightning. As lightening is a common enemy to equipments, it must be prevented as far as it can. There are generally two aspects of lightening which damage the equipment, direct and indirect hits.

Direct hits

Communication towers should be equipped with Franklin rods(lightening protectino unit) that are properly grounded at the base of the tower. However, if the lightening hits the tower itself. There will be chance that equipment will be saved.

Indirect hits

Induction currents (indirect hits) though nearby lightning strike can cause damage to outdoor radio equipment. That can be prevented by using surge protectors to vulnerable equipment and radio equipment with surge protectors is recommended to be used on the links. Those radio surge protectors protect only the radio.

Tools

Tools that can come handy are: climbing gear, walkie-talkie, ladders, backpackers, GPS equipment, maps, tripmeter, binoculars, blinking lamp or torch, ropes, tape and a standard tool box.

Local transport

Implementation of project is always in great need of transprt facility for equipment. Depending on the size of the team, the equipment, number of sites and distances between them, transprot facility should be budgeted.

Licences and permissions

As per the regulation of country/region adequate licenses and permissions might be necessary work for that location. So obtaining that before project is recommended.

Here are some general permission that's need to be taken care according to region

- Permission(s) to build a tower or mount an antenna
- Permission (includes license) to operate IEEE 802.11
- Permission to occupy the land and house/shelter
- Permission for the technical assistance

Mast or Tower

Mount the antenna on the top of a house or in an existing tower, we must of course contact the owner for permission. Errect a new tower/mast, we must ask for permission from the plot owner or authority.

If the tower or the top of the antenna is over a certain height (higher than the average landscape on the location) we need permission from the authority that regulates the airspace for that location.

Permission to operate IEEE 802.11/Frequency

On some country/region 2.4GHz or 5.8 GHz frequency band **may require a license though it is free to use according to ITU.**

Do not assume that what is free in one country should be free in your country. Normally it is the Commission for Communication (or similar) that handles the licenses for this type of communication.

The term "unlicensed frequency" can be misleading. Unlicensed does mean that a radio license is not needed to operate equipment at that frequency, but it does NOT mean transmit power is unregulated, means that the maximum power output must be not greater than a certain value (Watt) including the gain of the antenna. Permissions to operate IEEE 802.11 vary a lot from country to country depending on regulation.

For example Nigerian Communications Commission (NCC) has kept the 2.4 GHz ISM band as unlicensed with a maximum power at the point of transmission to be 1 Watt or 30 dBm. But in America it is only 20dBm.

Procurement of equipment

The procurement can be done locally (within the country) or import. The choice should depend on bandwitdh, range, support, operating frequency, avaibality. Price may be a key factor of radio procurement. And also one of the issue in procurement is Delivery time. This is a factor (unknown in many cases) that can delay a project quite implementation or testing.

Local Procurement

Procurement of any good equipment should always be done locally when it is suitable in terms of availability and support. Since overseas transport is very costly, and normally is charged by weight or volume, heavy and bulky equipment should preferable be procured locally.

Advanced radio equipment might sometimes be needed to import if not available locally.

Implementation Phase

Final phase is implementatino phase. By this time, we should already have the licences that we need. Also, all tools that are needed should be procured or leased.

This section discusses a few practical issues which will help on implementation phase.

Weather

- Installations in towers should be avoided during rainy seasons and in frequent lightning time.
- While choosing outdoor mounted equipment need to have an operating temperature range up to 70°C.
- When planning for the actual implementation we should consider the weather conditions for that that time of the year. In countries around the equator, we typically want to avoid the hottest season and the rain periods,while in Europe for example, we rather avoid the cold and wet winter for project implementation.

Quality assurance

Quality assurance is the process of evaluating, testing and measuring the overall project performance to verify that the requirements set up in the contract.

Depending on whether we are the consultant or if we are the client, there are certain things that we should focus on. As a consultant, what can we guarantee to your client in terms of performance, quality and sustainability? As the client, what do we demand from the consultant in terms of performance, quality and sustainability? These questions need to be carefully addressed in the contract to avoid future conflicts. To assure a certain level of quality, we need to agree on what quality is in that specific case and how it can be measured. For a wireless link the following parameters can be measured and indicate a certain level of quality:

- Uptime
- Jitter
- Throughput
- SNR
- Packet loss
- Duplicates of packets
- Round-trip time

The exact method of measuring the specific data is most importance.

The measurements should be done several times under different weather and load conditions. For example, a dry sunny day compared to a humid rainy day will change your measurements of the SNR. Also, measures taken during a weekend can differ from the ones taken during the week.

Being the client, we should carefully read the specifications of the equipment so that we are certain about that the specified hardware is suitable for your implementation. Check labels and compare the specifications. We should also make sure to include in the contract a period of time that the implementation should guarantee level of performance, other factor like support.

Networking Basics

This unit details the OSI/Internet protocol stack with focus on the issues that are critical in wireless network implementations. The unit also outlines the effect of every layer in the overall performance of a wireless communication network; aims to give an understanding of how the different layers (components) of the OSI model affect each other and targets the key elements that need to be considered when performing network planning. The OSI model is used as a "reference" that helps us to describe those interactions between components.

The OSI model

The OSI *(Open Systems Interconnection)* Reference Model, created by ISO (International Standards Organization), is an abstract description for computer network (communication) protocol design. The model splits different communication functions in seven different layers that can work independent of each other.

A protocol design that follows the structure of the OSI model follows the principles of a *'stack'.* Having a *layered* or *stack* protocol model implies that each layer only uses the functionality of the layer below and only provides functionality to layers above. A protocol 'stack' can be implemented in either software, hardware or a combination of both.

In many well known protocols the OSI model is not strictly followed in practice. For example, the Internet follows instead a four (4) level protocol suite consisting of Media Access Control Layer (link layer), Network Layer (IP), Transport Layer (TCP/UDP) and Application Layer.

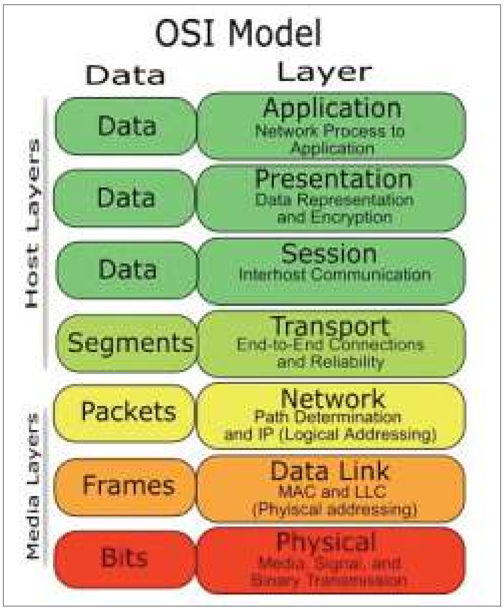

OSI Model
Data
Layer
Host Layers
Media Layers
Data
Application
Network Process to Application
Data
Presentation
Data Representation and Encryption
Data
Session
Interhost Communication
Segments
Transport
End-to-End Connections and Reliability
Packets
Network
Path Determination and IP (Logical Addressing)
Frames
Data Link
MAC and LLC (Phyiscal addressing)
Bits
Physical
Media, Signal, and Binary Transmission

Figure 4.1: OSI Model

OSI model versus TCP/IP protocol suite.

Wireless standards normally refer to layer 1 and layer 2 of the OSI protocol stack, keeping the IP packet unaltered. The "IP packets" are transported over a **wireless specific** physical and data link protocols.

Wireless standards (IEEE 802.11, IEEE 802.16, Bluetooth, IrDA etc...) deal with physical and data link layers only and have been traditionally designed to carry all types of data. IP is just one of the types of data. Wireless standards are designed outside of the Internet Engineering Task Force (IETF).

Media Access Control

The Media Access Control (MAC) layer in the TCP/IP model includes the OSI's *physical layer* that relates to the most physical aspects of the communication (modulation techniques, bit encoding, physical access to the share media etc) and the *link layer* protocol that is responsible for addressing and delivering packets from one computer (host) to another on a common shared channel.

In simple words, the physical layer is responsible of converting physical electromagnetic signals into bits, while the link layer is responsible of collecting those bits in a form of data packet.

Common physical layer protocols are RS-232, V.35, 10BASET, ISDN etc.,
Common link layer protocols are Ethernet (IEEE 802.3), PPP, ATM etc.

Wireless networks protocols as IEEE 802.11 (WLAN) refers to both the physical and link level layers of the OSI model. IEEE 802.11 family of protocols implements different physical (PHY) layer protocols based on spread spectrum (FHSS, DSSS, and OFDM).

The original standard IEEE 802.11 specifies a single Medium Access Control (MAC) layer and 3 Physical Layer Specifications. The standard provides 2 Physical layer specifications for radio, operating in the 2 400 - 2 483.5 MHZ band (FHSS and DSSS) and one for infrared.

Access control protocols

Carrier Sense Multiple Access (CSMA) and Collision Detection (CD)

The most popular physical access control mechanism where a set of computers access a common shared media is **Ethernet.** Ethernet protocol or IEEE 802.3 uses an access control protocol known as *Carrier Sense Multiple Access* (CSMA), which is an improved version of a contention technique scheme known as ALOHA.

When a node has data to transmit, it first listens to the media to see if any other node on the network is sending (by listening to the shared channel). If no other transmission is detected, the data is sent. It is possible and not uncommon that two different nodes can send data simultaneously since they both can detect an idle medium. In the case that multiple senders send data at the same time, a collision will occur and the data will be corrupted. The collision will be detected by the receiver since the CRC field in the MAC header will not match the existing payload. Corrupted data is discarded by the receiver.

Collision Detection (CD) is a second element of the Ethernet access protocol and is used by the sender to detect collisions. Nodes that are transmitting data can simultaneously monitor the shared media (they can listen what is in the media while sending). If a collision is detected (the node listens to something different from what was sent) the node stops the transmission and sends out a jam sequence to ensure receiving nodes that a collision has taken place and any recently packet should be dropped.

After a detected collision, all nodes will retransmit the data. To prevent the retransmissions colliding one more time, Ethernet uses a random back-off period (based on a random coefficient and the number of earlier retransmission) in order to calculate the time to wait for next transmission. Ethernet tries to minimize the probability of “re collisions” after collision detection.

IEEE 802.11 (WLAN)

The MAC layer of IEEE 802.11 (WLAN) is called CSMA/CA. It has lot similarities with Ethernet, it uses CSMA to share media over wireless nodes but lacks collision detection (CD). The sender can not detect a collision, as the data in the media can not be “listened” while sending. IEEE 802.11 operates in half duplex (send/receive) by using a TDD scheme. Collision detection, as is employed in Ethernet, cannot be used for the radio frequency transmissions of IEEE 802.11
Since nodes can detect idle media but can not detect collisions in wireless media, the access point needs to send an acknowledgement to ensure a successful transmission instead. This mechanism creates an overhead and reduces the useful data throughput.

Due to these limitations, a well known problem occurs in point to IEEE 802.11b multipoint configurations, the “hidden node” problem. In a point to multipoint configuration, a set of nodes talk to a common node named “Access Point”. A “hidden node” is caused by the fact that all nodes can not hear each other in a wireless network and collisions are unavoidable using just “CSMA.” To solve (or ease) the problem the MAC layer of IEEE 802.11 includes a mechanism call Collision Avoidance (CA). When using CA, a transmitting node needs to send a RTS (request to send) packet to the access point and wait for a CTS (clear to send) before starting the transmission.

Even though all nodes might not be able to hear the RTS packet send by other nodes, they can always hear the CTS packet sent by the access point address to a given node. Hence, the nodes can avoid sending data during the time allocated by the access point to another node. When the number of nodes in the network and the distance between the nodes and access point increases, RTS/CTS does not scale and other alternatives to IEEE 802.11b are needed.

MAC Addressing

A MAC address is used in the link layer as the mechanism to identify and address data traffic to host in a shared media. It consists of a universally unique sequence of 48-bits (12 hex digit) associated with a particular wireless network interface (device).

When a data packet is sent over a shared media, the source and destination of the computers (hosts) are included in the header of the packet. When a packet needs to be send to all hosts (broadcast), a special MAC address is used, in Ethernet the broadcast MAC address is ff:ff:ff:ff:ff:ff (all 48 bits to 1)

In normal circumstances, the network interface cards (NIC) only pass to the Operative System the data packets that match the MAC address of the computer.

The MAC address is normally hardware coded when shipped from the vendor.

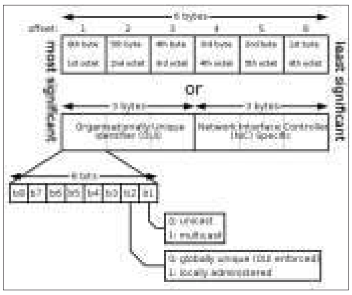


Figure 4.2: MAC Address

Using MAC addresses for authentication

It has become very common in many wirelesses ISPs (WISP) to use the MAC address of the wireless interface as a mechanism to limit/provide access to a wireless network. The assumption is that MAC addresses are “hard-coded” and can not be modified by normal users. The reality is different and MAC addresses in most (wireless) network interfaces can easily be modified.

Link level encryption

Link level encryption is the process to secure data at the link level when data is transmitted between two nodes attached to the same physical link (they can also be in two different physical links by means of a repeater e.g. Satellite). Any other protocols or application data running over the physical link are protected from eavesdroppers.

Encryption requires a certain key or secret shared between the communication parties and an agreed encryption algorithm. When the sender and the receiver are not present in the same media the data needs to be decrypted and reencrypted in each of the node along the way to the receiver. The link level encryption is normally used when higher level protocol encryption is not present.

Link level encryption in IEEE 802.11

The best known link level encryption algorithm for IEEE 802.11 is the so called Wired Equivalent Privacy (WEP). Now WEP treated as insecure and other higher level of encryption is proposed and standardized as the Wi-Fi Protected Access (WPA). The new standard IEEE 802.11i will include an enhancement of WPA, named WPA-2. Link encryption does not provide end-to-end security outside of the physical link and should always be consider as just an extra security measure in your network design.

Network layer (IP)

The IP (Internet Protocol) layer is a protocol used to transmit data across a packet-switched network. Data sent over an IP network is referred as packets (or datagrams). The IP protocol provides an best service (best effort) on packet transfer. Packets can arrive damaged, duplicated, and out of order or be entirely discarded by any host along the path.

An important part of the IP protocol, is the source and destination address of the communicating parties. That information (the addresses) is not only used to route packets, identify Internet hosts but is also required by higher level applications as firewalls.

Addressing

The commonly used IP protocol is IPv4 which uses a 32-bit field for addressing.
Ipv4 Address Basics
IPv4 addresses are 32 bits, organized into four groups of 8 bits called octets or bytes.

They are shown in decimal (base 10) usually, with each octet converted to decimal, separated by a period. Each octet can be from 0 to 255 decimal (00000000 to 11111111 binary).

Examples:

1. 192.16.3.3
2. 199.99.125.16
3. 38.2.131.1
4. 144.118.28.254
5. 128.122.159.3

IP addresses are organized into address classes that separate the network and host portions.
Converting binary to decimal
Remember (or calculate) the powers of two from 20 to 27

128	64	32	16	8	4	2	1
27	26	25	24	23	22	21	20

To convert binary to decimal: place the octet against the powers of two and add the powers of two where there is a 1 in the binary number

Example: convert 11000111 to decimal:

128	64	32	16	8	4	2	1
1	1	0	0	0	1	1	1

So 11000111 binary equals decimal 128 + 64 + 4 + 2 + 1 = 199.

Now convert 01011001 to decimal:

128	64	32	16	8	4	2	1
0	1	0	1	1	0	0	1

So 01011001 binary equals decimal 64 + 16 + 8 + 1 = 89.

Convert decimal to binary

Find the highest power of two that can be subtracted from the number. Put a 1 in that position. Subtract it from the number and repeat the process. Put in zeroes for all the positions not used.

Example: convert 199 to binary.

Highest number is 128:

128	64	32	16	8	4	2	1
1							

199-128 = 71 highest number remaining: 64

128	64	32	16	8	4	2	1
1	1	0	0	0	0	0	0

71-64 = 7 highest number remaining = 4 (place zeroes for the others)

128	64	32	16	8	4	2	1
1	1	0	0	0	1		

7-4 = 3 highest number 2

128	64	32	16	8	4	2	1
1	1	0	0	0	1	1	

3-2 = 1 highest number 1

128	64	32	16	8	4	2	1
1	1	0	0	0	1	1	1

Network and host portions

Normally host portion is denoted as zero and network portion as its own number.

Example network numbers:

206.4.23.0 is an example of a class C network number. Last 8 bits are set to zero.

128.122.0.0 is an example of a class B network number. Last 16 bits are set to zero. Where underlined portion of the ip address is network portion of a network and remaining is host portion.

Network Masks

A network mask indicates which portion of the address identifies the network and which portion of the address identifies the node. Class A, B, and C networks have default masks, also known as natural masks, as shown here:

Class A	255.0.0.0
Class B	255.255.0.0
Class C	255.255.255.0

An IP address on a Class A network that has not been subnetted would have an address/mask pair similar to: 8.20.15.1 255.0.0.0. To see how the mask helps you identify the network and node parts of the address, convert the address and mask to binary numbers.

8.20.15.1	00001000.00010100.00001111.00000001
255.0.0.0	11111111.00000000.00000000.00000000

Once you have the address and the mask represented in binary, then identifying the network and host ID is easier. Any address bits which have corresponding mask bits set to 1 represent the network ID. Any address bits that have corresponding mask bits set to 0 represent the node ID.

8.20.15.1 = 00001000.00010100.00001111.00000001
255.0.0.0 = 11111111.00000000.00000000.00000000

net id host id

netid = 00001000 = 8
hostid = 00010100.00001111.00000001 = 20.15.1

Subnetting

Subnetting allows you to create multiple logical networks that exist within a single Class A, B, or C network. If you do not subnet, you are only able to use one network from your Class A, B, or C network, which is not recomended.

Subnetting allows you to create multiple logical networks that exist within a single Class A, B, or C network. If you do not subnet, you are only able to use one network from your Class A, B, or C network, which is not recomended.

In order to subnet a network, extend the natural mask using some of the bits from the host ID portion of the address to create a subnetwork ID. For example, given a Class C network of 204.17.5.0 which has a natural mask of 255.255.255.0, you can create subnets in this manner:

204.17.5.0 - 11001100.00010001.00000101.00000000

255.255.255.224 - 11111111.11111111.11111111.11100000

-------------------------|sub|----

By extending the mask to be 255.255.255.224, you have taken three bits (indicated by "sub") from the original host portion of the address and used them to make subnets. With these three bits, it is possible to create eight subnets. With the remaining five host ID bits, each subnet can have up to 32 host addresses, 30 of which can actually be assigned to a device since host ids of all zeros or all ones are not allowed (it is very important to remember this). So, with this in mind, these subnets have been created.

204.17.5.0 255.255.255.224	host address range 1 to 30
204.17.5.32 255.255.255.224	host address range 33 to 62
204.17.5.64 255.255.255.224	host address range 65 to 94
204.17.5.96 255.255.255.224	host address range 97 to 126
204.17.5.128 255.255.255.224	host address range 129 to 158
204.17.5.160 255.255.255.224	host address range 161 to 190
204.17.5.192 255.255.255.224	host address range 193 to 222
204.17.5.224 255.255.255.224	host address range 225 to 254

Note: There are two ways to denote these masks. First, since you are using three bits more than the "natural" Class C mask, you can denote these addresses as having a 3-bit subnet mask. Or, secondly, the mask of 255.255.255.224 can also be denoted as /27 as there are 27 bits that are set in the mask. This second method is used with CIDR. Using this method, one of these networks can be described with the notation prefix/length. For example, 204.17.5.32/27 denotes the network 204.17.5.32 255.255.255.224. When appropriate the prefix/length notation is used to denote the mask throughout the rest of this document.

The network subnetting scheme in this section allows for eight subnets, and the network might appear as:

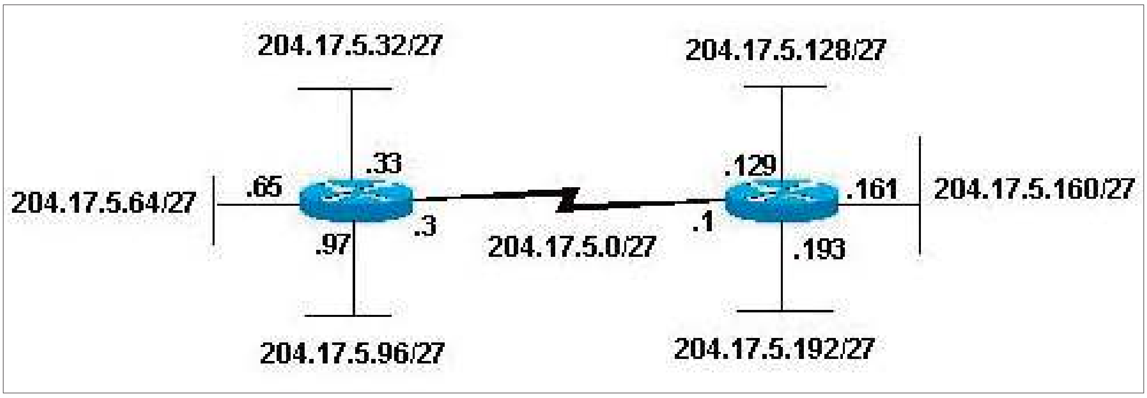


Figure 4.3: showing subnets

Notice that each of the routers in above Figure is attached to four subnetworks, one subnetwork is common to both routers. Also, each router has an IP address for each subnetwork to which it is attached. Each subnetwork could potentially support up to 30 host addresses.

`This brings up an interesting point. The more host bits you use for a subnet mask, the more subnets you have available. However, the more subnets available, the less host addresses available per subnet. For example, a Class C network of 204.17.5.0 and a mask of 255.255.255.224 (/27) allows you to have eight subnets, each with 32 host addresses (30 of which could be assigned to devices). If you use a mask of 255.255.255.240 (/28), the break down is:

204.17.5.0 - 11001100.00010001.00000101.00000000
255.255.255.240 - 11111111.11111111.11111111.11110000

--------------------------|sub |---

Since you now have four bits to make subnets with, you only have four bits left for host addresses. So in this case you can have up to 16 subnets, each of which can have up to 16 host addresses (14 of which can be assigned to devices).

Take a look at how a Class B network might be subnetted. If you have network 172.16.0.0 ,then you know that its natural mask is 255.255.0.0 or 172.16.0.0/16. Extending the mask to anything beyond 255.255.0.0 means you are subnetting. You can quickly see that you have the ability to create a lot more subnets than with the Class C network. If you use a mask of 255.255.248.0 (/21), how many subnets and hosts per subnet does this allow for?

172.16.0.0 - 10101100.00010000.00000000.00000000
255.255.248.0 - 11111111.11111111.11111000.00000000

-----------------| sub |-----------

You are using five bits from the original host bits for subnets. This allows you to have 32 subnets (25). After using the five bits for subnetting, you are left with 11 bits for host addresses. This allows each subnet so have 2048 host addresses (211), 2046 of which could be assigned to devices.

Note: In the past, there were limitations to the use of a subnet 0 (all subnet bits are set to zero) and all ones subnet (all subnet bits set to one). Some devices would not allow the use of these subnets. Cisco Systems devices allow the use of these subnets when theip subnet zero command is configured.

Examples

Sample Example 1

Now that you have an understanding of subnetting, put this knowledge to use. In this example, you are given two address / mask combinations, written with the prefix/length notation, which have been assigned to two devices. Your task is to determine if these devices are on the same subnet or different subnets. You can do this by using the address and mask of each device to determine to which subnet each address belongs.

DeviceA: 172.16.17.30/20
DeviceB: 172.16.28.15/20

Determining the Subnet for DeviceA:

172.16.17.30 - 10101100.00010000.00010001.00011110
255.255.240.0 - 11111111.11111111.11110000.00000000

-----------------| sub|------------

subnet = 10101100.00010000.00010000.00000000 = 172.16.16.0

Looking at the address bits that have a corresponding mask bit set to one, and setting all the other address bits to zero (this is equivalent to performing a logical "AND" between the mask and address), shows you to which subnet this address belongs. In this case, DeviceA belongs to subnet 172.16.16.0.

Determining the Subnet for DeviceB:

172.16.28.15 - 10101100.00010000.00011100.00001111
255.255.240.0 - 11111111.11111111.11110000.00000000

-----------------| sub|------------

subnet = 10101100.00010000.00010000.00000000 = 172.16.16.0

From these determinations, DeviceA and DeviceB have addresses that are part of the same subnet.

Sample Example

Given the Class C network of 204.15.5.0/24, subnet the network in order to create the network in Figure given below with the host requirements shown.

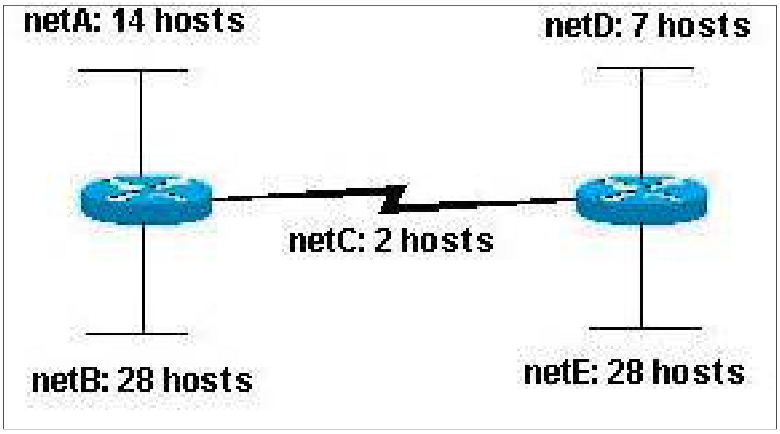


Figure 4.4: showing different subnets with different number of hsot

Looking at the network shown in given figure, you can see that you are required to create five subnets. The largest subnet must support 28 host addresses. Is this possible with a Class C network? and if so, then how?

You can start by looking at the subnet requirement. In order to create the five needed subnets you would need to use three bits from the Class C host bits. Two bits would only allow you four subnets (22).

Since you need three subnet bits, that leaves you with five bits for the host portion of the address. How many hosts does this support? 25 = 32 (30 usable). This meets the requirement.

Therefore you have determined that it is possible to create this network with a Class C network. An example of how you might assign the subnetworks is:

netA: 204.15.5.0/27	host address range 1 to 30
netB: 204.15.5.32/27	host address range 33 to 62
netC: 204.15.5.64/27	host address range 65 to 94
netD: 204.15.5.96/27	host address range 97 to 126
netE: 204.15.5.128/27	host address range 129 to 158

VLSM (Variable Length Subnet Mask)

In all of the previous examples of subnetting, notice that the same subnet mask was applied for all the subnets. This means that each subnet has the same number of available host addresses. You can need this in some cases, but, in most cases, having the same subnet mask for all subnets ends up wasting address space. For example, in the Sample example 2 section, a class C network was split into eight equal-size subnets; however, each subnet did not utilize all available host addresses, which results in wasted address space. Figure below illustrates this wasted address space.

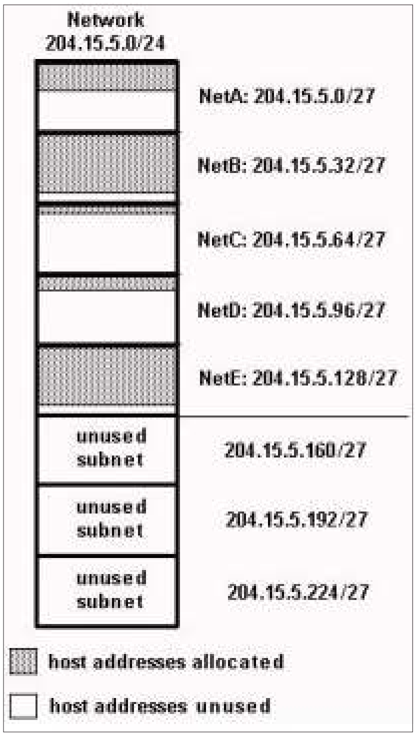


Figure: 4.5: Showing VLSM network block

Figure illustrates that of the subnets that are being used, NetA, NetC, and NetD have a lot of unused host address space. It is possible that this was a deliberate design accounting for future growth, but in many cases this is just wasted address space due to the fact that the same subnet mask is being used for all the subnets.

Variable Length Subnet Masks (VLSM) allows you to use different masks for each subnet, thereby using address space efficiently.

VLSM Example

Given the same network and requirements as in Sample Example 2 develop a subnetting scheme with the use of VLSM, given:

netA:	must support 14 hosts
netB:	must support 28 hosts
netC:	must support 2 hosts
netD:	must support 7 hosts
netE:	must support 28 host

Determine what mask allows the required number of hosts.

netA:	requires a /28 (255.255.255.240) mask to support 14 hosts
netB:	requires a /27 (255.255.255.224) mask to support 28 hosts
netC:	requires a /30 (255.255.255.252) mask to support 2 hosts
netD*:	requires a /28 (255.255.255.240) mask to support 7 hosts
netE:	requires a /27 (255.255.255.224) mask to support 28 hosts

* a /29 (255.255.255.248) would only allow 6 usable host addresses
therefore netD requires a /28 mask.

The easiest way to assign the subnets is to assign the largest first. For example, you can assign in this manner:
netB: 204.15.5.0/27 host address range 1 to 30
netE: 204.15.5.32/27 host address range 33 to 62
netA: 204.15.5.64/28 host address range 65 to 78
netD: 204.15.5.80/28 host address range 81 to 94
netC: 204.15.5.96/30 host address range 97 to 98

This can be graphically represented as shown in Figure 5:

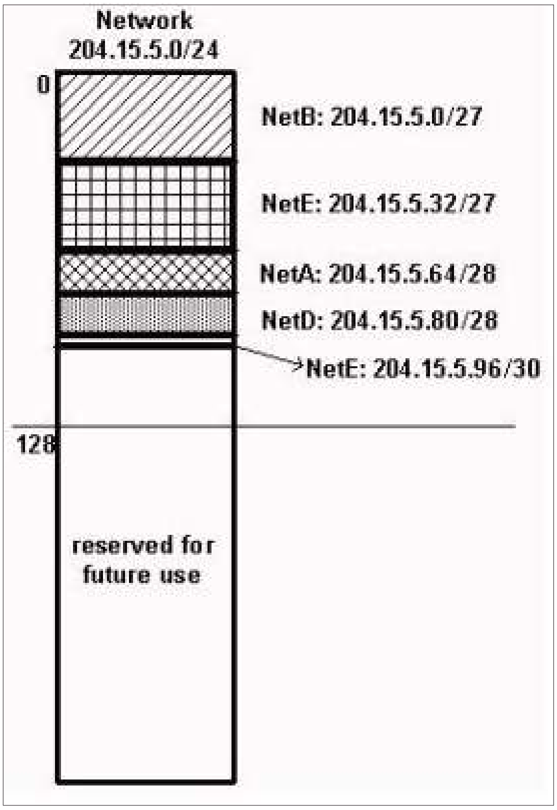


Figure4.6: VLSM with different block size

This figure illustrates how using VLSM helped save more than half of the address space.

CIDR (Classless Interdomain Routing)

Classless Interdomain Routing (CIDR) was introduced to improve both address space utilization and routing scalability in the Internet. It was needed because of the rapid growth of the Internet and growth of the IP routing tables held in the Internet routers.

CIDR moves way from the traditional IP classes (Class A, Class B, Class C, and so on). In CIDR , an IP network is represented by a prefix, which is an IP address and some indication of the length of the mask. Length means the number of left-most contiguous mask bits that are set to one. So network 172.16.0.0 255.255.0.0 can be represented as 172.16.0.0/16. CIDR also depicts a more hierarchical Internet architecture, where each domain takes its IP addresses from a higher level. This allows for the summarization of the domains to be done at the higher level. For example, if an ISP owns network 172.16.0.0/16, then the ISP can offer 172.16.1.0/24, 172.16.2.0/24, and so on to customers. Yet, when advertising to other providers, the ISP only needs to advertise 172.16.0.0/16.

Types of IPv4 addresses

The Internet standards define the following types of IPv4 addresses:

Unicast: Used for one-to-one communications.
Multicast: Used for one-to-many communications.
Broadcast: Used for one-to-everyone-on-a-subnet communications.

IPv4 unicast addresses

The IPv4 unicast address identifies an interface's location on the network in the same way a street address identifies a house on a city block. Just as a street address must identify a unique residence, an IPv4 unicast address must be globally unique to the network and have a uniform format.

Each IPv4 unicast address includes a network ID and a host ID.

- The network ID (also known as a network address) is the fixed portion of an IPv4 unicast address that identifies the set of interfaces that are located on the same physical or logical network segment as bounded by IPv4 routers.
  A network segment on TCP/IP networks is also known as a subnet. All systems on the same physical or logical subnet must use the same network ID and the network ID must be unique to the entire TCP/IP network.
- The host ID (also known as a host address) is the variable portion of an IPv4 unicast address that is used to identify a network node's interface on a subnet. The host ID must be unique to the network ID.
- If the network ID is unique to the TCP/IP network and the host ID is unique to the network ID, then the entire IPv4 unicast address consisting of the network ID and host ID is unique to the entire TCP/IP network.

IPv4 multicast addresses

IPv4 multicast addresses are used for single-packet, one-to-many delivery. On an IPv4 multicast-enabled intranet, an IPv4 packet addressed to an IPv4 multicast address is forwarded by routers to the subnets on which there are hosts listening to the traffic sent to the IPv4 multicast address. IPv4 multicast provides an efficient one-to-many delivery service for many types of communication.

IPv4 multicast addresses are defined by the class D Internet address class: 224.0.0.0/4. IPv4 multicast addresses range from 224.0.0.0 through 239.255.255.255. IPv4 multicast addresses for the 224.0.0.0/24 address prefix (224.0.0.0 through 224.0.0.255) are reserved for local subnet multicast traffic.

IPv4 broadcast addresses

IPv4 uses a set of broadcast addresses to provide a one-to-everyone-on-the-subnet delivery service. Packets sent to IPv4 broadcast addresses are processed by all the interfaces on the subnet. The following are the different types of Ipv4 broadcast addresses:

- **Network broadcast.** Formed by setting all the host bits to 1 for a classful address prefix. An example of a network broadcast address for the classful network ID 131.107.0.0/16 is 131.107.255.255. Network broadcasts are used to send packets to all interfaces of a classful network. IPv4 routers do not forward network broadcast packets.

- **Subnet broadcast.** Formed by setting all the host bits to 1 for a classless address prefix. An example of a network broadcast address for the classless network ID 131.107.26.0/24 is 131.107.26.255. Subnet broadcasts are used to send packets to all hosts of a classless network. IPv4 routers do not forward subnet broadcast packets. For a classful address prefix, there is no subnet broadcast address, only a network broadcast address. For a classless address prefix, there is no network broadcast address, only a subnet broadcast address.

- **All-subnets-directed broadcast.** Formed by setting all the original classful network ID host bits to 1 for a classless address prefix. A packet addressed to the all-subnets-directed broadcast was defined to reach all hosts on all of the subnets of a subnetted class-based network ID. An example of an all-subnets-directed broadcast address for the subnetted network ID 131.107.26.0/24 is 131.107.255.255. The all-subnets-directed broadcast is the net work broadcast address of the original classful network ID. IPv4 routers can forward all-subnets-directed broad cast packets, but the use of the all-subnets-directed broadcast address is deprecated in RFC 1812.

- **Limited broadcast.** Formed by setting all 32 bits of the IPv4 address to 1 (255.255.255.255). The limited broad cast address is used for one-to-everyone delivery on the local subnet when the local network ID is unknown. Ipv4 nodes typically only use the limited broadcast address during an automated configuration process such as Boot strap Protocol (BOOTP) or DHCP. For example, with DHCP, a DHCP client must use the limited broadcast address for all traffic sent until the DHCP server acknowledges the use of the offered IPv4 address configuration. IPv4 routers do not forward limited broadcast packets.

More about Ipv4 Addresse Block

127.0.0.0/8 - This block is assigned for use as the Internet host loopback address. A datagram sent by a higher level protocol to an address anywhere within this block loops back inside the host. This is ordinarily implemented using only 127.0.0.1/32 for loopback. As described in [RFC1122], Section 3.2.1.3, addresses within the entire 127.0.0.0/8 block do not legitimately appear on any network anywhere.

169.254.0.0/16 - This is the "link local" block. As described in [RFC3927], it is allocated for communication between hosts on a single link. Hosts obtain these addresses by auto-configuration, such as when a DHCP server cannot be found.

172.16.0.0/12 - This block is set aside for use in private networks. Its intended use is documented in [RFC1918]. As described in that RFC, addresses within this block do not legitimately appear the public Internet. These addresses can be used without any coordination with IANA or an Internet registry.

192.168.0.0/16 - This block is set aside for use in private networks. Its intended use is documented in [RFC1918]. As described in that RFC, addresses within this block do not legitimately appear the public Internet. These addresses can be used without any coordination with IANA or an Internet registry.

224.0.0.0/4 - This block, formerly known as the Class D address space, is allocated for use in IPv4 multicast address assignments. The IANA guidelines for assignments from this space are described in [RFC3171]

Ipv6. The next generation of IP protocol uses 128-bit source and destination addresses to avoid the fact that Ipv4 are running out of available addresses.

Subnetting in wireless networks

It is a common practice in many wireless ISPs not to subnet their networks properly. A big subnet without many routing decisions is very easy to deploy it is not recommended networks grow, troubleshooting is far more complex and time consuming.

Good subnetting and routing design in the wireless network limits the amount of useless broadcast traffic and probes to scale better.

Avoid the use of one single big subnet as much as possible. Limiting the subnets host size to 32-64 is recommended.

Error control

Error control is handled by a set of control messages at the IP level, ICMP (Internet Control Message Protocol). The protocol does not provide extensive error control but merely reports error to the originating hosts.

Two of the main uses of ICMP are the following types of operations.
Report problems that prevents delivery (such as **"Destination Unreachable"**)

Troubleshooting the network through use of request and reply messages (such as "Echo Request" and "Echo Reply" used by ping)

An ICMP, error message; always contains the full IP header (including options) of the IP datagram that failed and the first eight bytes of the IP data field. The error can therefore be associated with a certain protocol and a particular process (from the port number in the TCP or UDP header which are the first eight bytes in the IP data field). P or UDP header which are the first eight bytes in the IP data field).

Monitoring ICMP in wireless networks

It will allow us to identify connectivity problems inside of your network

Routing

The process of transfer a packet of data from source to destination is called routing. A routing decision is made in each computer between the source and destination to determine the most suitable next hop towards the target machine. The routing decision is specified in the routing table.

All common routing algorithms use either the destination or source of the IP address. In the first case the route is determined by looking at the destination address of the packet (most commonly used) while the second one uses the source address to determine the path to the target. A third option is known as “policy-based routing”, where routing decisions are dependent on other sources of information (MAC address, type of service, network load etc.).

NAT (Network Address Translation)

NAT as a general concept is the capability of a router to “rewrite” the source or destination address of an IP packet (datagram). NAT became popular because it allows single device with a public IP address to represent a group of computers in a private network.

NAT is not only useful when there is a shortage of public IP addresses but also as a mechanism to implement other network functions:

- Firewall / DMZ
- Traffic load balance (e.g. identical web servers behind a NAT to balance requests)
- Computing load balance (e.g. identical databases to balance computing load of queries)

Masquerading - SNAT

IP masquerading or Source NAT allows hosts with private IP addresses to communicate with hosts outside their own network by letting one machine act on others behalf. IP masquerading is a simple and limited form of a firewall. Masquerading does not allow a host to initiate a connection to another host inside of the network.

Masquerading rewrites the source address of the packets as they pass through router, so that the target machine always sees the router itself as a sender. When the recipient of traffic answers back, the router rewrite the destination address to the original sender. Masquerading adds some level of security by acting as a type of firewall but also limits the users inside a network to provide services outside the network.

NB In a pure sense, MASQUERADE is not identical to SNAT, since masquerading flushes previous connections when the interface goes down or changes IP address.

Destination NAT - DNAT

DNAT (Destination Network Address Translation) is commonly used to make a service publicly available from an internal network (private IP address) through rewriting the destination IP address of the packet.

DNAT can be used to route traffic inside of a DMZ. The DMZ or Demilitarized Zone is the area of a network that is dedicated to host public services. The DMZ is normally placed in another network segment isolated from other transit traffic.

By using DNAT we can redirect (map) incoming traffic to a certain public IP address and port number to one IP address and port number of the DMZ.

NAT configuration on Cisco Router

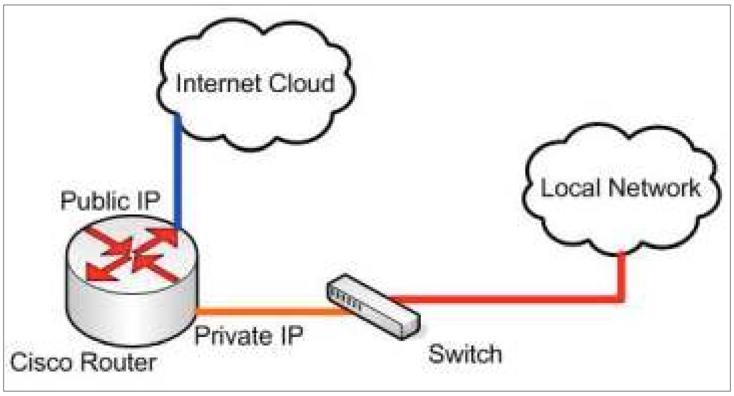


Figure4.7: Routing Example

NAT on your Cisco router, follow these simple steps.

1. Identify your outside (public) interface.
2. Identify your inside (private) interface.
3. Specify what IP netblock you want to NAT or NAT all subnets.
4. Enter the configuration of Cisco router

Step,

i. Configure terminal ### This command will get to configuration ####
ii. Interface <public> <interference number >

Example interface FastEthernet 0/0

iii. ip nat outside
iv. end
v. interface <private> <interference number>

Example: interface FastEthernet 0/1

vi. ip nat inside
vii. end
viii. access-list 1 permit <private ip range>

Examples: access-list 1 permit 192.168.10.0 0.0.0.255 any

ix. access-list 1 premit any any
x. ip nat inside source list 1 interface <public interface > overload

Example ip nat inside source list 1 interface FastEthernet 0/0 overload

5. For verification we can use following command "show ip nat translations"

Pro Inside global	Inside local	Outside local	Outside global tcp
200.2.2.1:53638	192.168.10.6:53638	64.233.189.99:80	64.233.189.99:80

6. If there is following type of output then the NAT is working or you can able to ping the next hop Public address to verify it.

Enabling Transparent Web Proxying with Cisco router

There are a number of good reasons for any network to deploy proxies for user access to the Internet. Amongst these are

- Monitoring of web sites and traffic volumes
- Restricting web access - by user, web sites, time of day, etc.
- Using caching to reduce traffic volumes
- Managing bandwidth

There are also a number of challenges faced when implementing proxies.

A Basic Network and Web proxy

In the network drawing below a basic network with access to the Internet, this is a very common configuration for small networks.

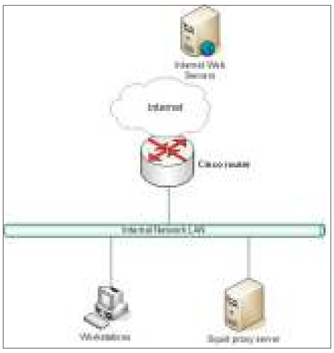


Figure 4.8: A basic network and proxy

A common solution for transparent proxying is to have all outbound traffic pass through a server which will detect web access and redirect the request to an internal proxy.

WCCP Overview

Most Cisco routers support a protocol called Web Cache Control Protocol, or WCCP. This protocol is used by a proxy server, such as a Linux server running the Squid proxy, to tell the router that it is alive and ready to process web access requests. WCCP uses the UPD protocol on port 2048 - it is essentially a one-way communication from the proxy to the router.

WCCP has a number of advantages when used between a proxy and the gateway router.

- You can have multiple proxy servers. In fact, you can have almost any number if your router is big enough to handle them. This means for large organisation the load will be spread amongst them improving performance.
- Access is resilient to failure. If a proxy fails, then the router will immediately start using another (if you've got more than one configured), otherwise it will stop using proxies and forward requests directly to the Internet. The router can also be configured to block Internet web access if there are no running proxies available.

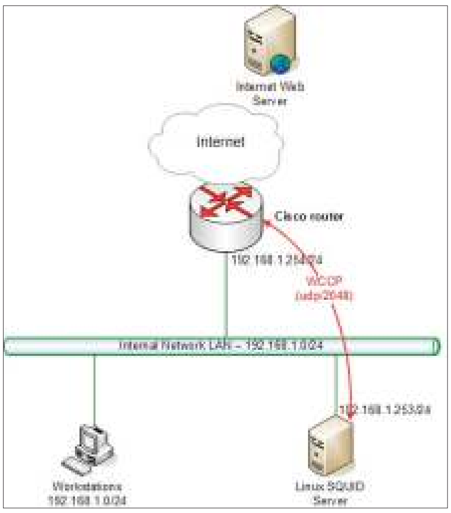


Figure 4.9: WCCP between the proxy and router

- Optimised hashing of URLs. When you have more than one proxy a user will request a web page that will then be cached by a proxy. The next time any user requests the same page, the router will send the request to the same proxy with the cached copy of the page.

One caveat here to note though : WCCP is patented by Cisco, and is generally only available on Cisco routers and some high-end Cisco switches.

WCCP proxy traffic flows are a little bit unusual, and can be very confusing to begin with. The following drawing shows the main flows for a WCCP proxy:

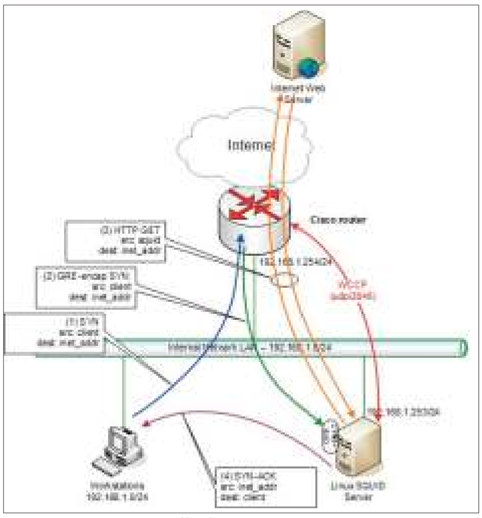

Internet Web Server
Internet
Cisco router
(3) HTTP GET src: squid dest: inet_addr
(2) GRE-encap SYN src: client dest: inet_addr
(1) SYN src: client dest: inet_addr
192.168.1.254/24
WCCP (udp/2048)
Internal Network LAN – 192.168.1.0/24
192.168.1.253/24
Workstations 192.168.1.0/24
(4) SYN-ACK src: inet_addr dest: client
Linux SQUID Server

Figure 4.10: WCCP traffic flows

There's some interesting things to note about the traffic flows here.

- The Squid proxy sends a WCCP packet to the router every 10 seconds to tell the router that the proxy is alive and ready to receive web requests. You can now see here that it is easy to have multiple proxy servers that can work with the router.
- When a client makes a request for an Internet web page, it sends it directly to the Internet via the outer, as shown in (4.6) above.
- The router captures the request, encapsulates it in a GRE packet, and forwards it to the proxy as shown in (4.7) above.
- The linux system un-encapsulates the GRE packet and sends the request to the Squid proxy by performing a Destination NAT operation on the packet - note that Squid now receives the original packet with its original source and destination IP addresses.
- The Squid proxy now fetches the web page from the Internet server in the normal fashion shown in (4.8) above - it uses its own IP address as the source and the original destination IP address for the destination. Note that the router does not intercept and attempt to proxy this request.
- Once Squid has downloaded the page, it saves the data in its own cache, then replies directly back to the client on the internal network. And this is the tricky thing right here - when Squid replies it uses the IP address of the In ternet server as the source in the packet, and the client IP address as the destination, this is shown in (4.9) above.

So, while the client thinks it is interacting with the remote web server via the Internet router, in actual fact it is interacting with the Squid proxy which is caching pages behind the scenes. If another user on another client makes a request for the same page they go through the same flow, but because the page is cached there is no need for Squid to fetch the page from the Internet server again.

In the remainder of this paper I will briefly show the Cisco, Linux, and Squid configurations required to get this working.

Cisco Configuration

In this example, I will have 2 proxies configured on the internal network (192.168.1.0/24) with IP addresses of 192.168.1.252 and 192.168.1.253. The first step is to define an access list containing the addresses of the proxies, and assign this as the list of WCCP proxies:

```
access-list 10 permit 192.168.1.252
access-list 10 permit 192.168.1.253
ip wccp web-cache group-list 10
```

Next we define another access-list to define direct or WCCP-proxied internet access. The proxies on 192.168.1.252 & 253 are denied access to WCCP, all other hosts on 192.168.1.0/24 are proxied when going to port 80, all others are denied. Denial implies direct access to the remote web server.

```
access-list 120 remark ACL for WCCP proxy access
access-list 120 remark Squid proxies bypass WCCP
access-list 120 deny ip host 192.168.1.253 any
access-list 120 deny ip host 192.168.1.252 any
access-list 120 remark LAN clients proxy port 80 only
access-list 120 permit tcp 192.168.1.0 0.0.0.255 any eq 80
access-list 120 remark all others bypass WCCP
access-list 120 deny ip any any
!
!
Assign ACL to WCCP
ip wccp web-cache redirect-list 120
Now set WCCP version 2:
ip wccp version 2
```

Verify the configuration - it should be active on version 2 with no caches connected until the Squid proxy is configured.

```
Router#sh ip wccp
```

Global WCCP information:

Router information:

```
Router Identifier:                -not yet determined-
Protocol Version:                 2.0
Service Identifier:               web-cache
Number of Service Group Clients:  0
Number of Service Group Routers:  0
Total Packets s/w Redirected:     0
Process:                          0
Fast:                             0
CEF:                              0
Redirect access-list:             120
Total Packets Denied Redirect:    0
Total Packets Unassigned:         0
Group access-list:                -none-
Total Messages Denied to Group:   0
Total Authentication failures:    0
Total Bypassed Packets Received:  0
Router#
```

At this point, client browsers which are not configured to use the Squid proxy explicitly may not be able to reach Internet web sites if the Squid proxy is registered with the router. If this is an issue for the users then the best option to disable & enable WCCP proxying is to remove the configuration from the interface (Fastethernet/0 in this case):

```
int f0
!
no ip wccp web-cache redirect in
```

and to enable it:

```
int f0
!
ip wccp web-cache redirect in
```

Manipulating traffic in a wireless network

NAT (SNAT/DNAT) can be used to manipulate traffic inside of a wireless network. While the users (hosts) of the network have the same settings, we can direct how their traffic is routed and which services are made available to them.

We can apply NAT to redirect web requests to a proxy server; furthermore we can also redirect different segments of the network to different web proxy servers attached to different Internet providers. NAT can also be used to redirect users to a captive portal where they have to register or enter their wireless account information.

IP tunnelling – IPSEC

IP tunneling is a method to transport IP packets inside of other IP packets to allow packets destined for one IP address to be redirected to another network first. Tunneling is the process of encapsulating IP packets. When the encapsulation is done inside of an encrypted IP packet, the IP tunneling is known as secure tunneling or VPN.

IP tunneling requires that the end-points of the tunnel are fully routable and not blocked by firewalls or NATs.

Using IP tunneling does not provide any added security if the encapsulated packet (the packet that travels inside) is not encrypted. The most common way to build secure IP tunneling is to use IPSEC.

IPSEC is a set of protocols that ensures security on the IP level. IPSEC supports secure IP encapsulation and provide certain security properties to all applications running at the top of IPSEC.

When it comes to security on IP level, there are 3 kind of protection that IPSEC can ensure:

- **Confidentiality** (protection of content)
- **Authentication** (verification of message sender)
- **Integrity** (content has not been forged)

To ensure those security properties, IPSEC uses three main protocols, in a nutshell:

Authentication Header (AH):

Provides strong Crypto checksum on the "whole" IP packet. A correct checksum in a received packet ensures that the packet was originated by the intended sender and has not been modified during transfer.

Encapsulating Security Payload (ESP): Provides strong encryption on the payload. A correct decrypted packet ensures the protection of the content of the packet. The packet was encrypted using a common shared secret between the communicating parties.

Internet Key Exchange (IKE): Provides different ways to negotiate keys session.

IPSEC in wireless networks

IPSEC requires end-to-end routability in a wireless networks. If we plan to deploy IPSEC, avoid the use of NATs and deploy full functional firewalls instead. IP encapsulation also includes an extra overhead, using IPSEC in conjunction with compression is recommended for optimization.

IPSEC requires the design of a proper key management. If a very limited set of parties are going to communicate with IPSEC, the most simple key distribution method is the use of symmetric keys. Unfortunately, perfect forward secrecy will not be guaranteed.

If we need to build VPNs inside of we wireless network we can also consider using Application Layer VPNs. Application layer VPNs normally use UDP tunneling and SSL protocol for encryption.

Transport Layer

The Transport Layer supports transfer of IP packets between processes (services) using ports (numbers). A TCP port is a logical connection that associates a certain transfer with a running process.

TCP (Transmission Control Protocol)

TCP (Transmission Control Protocol) is a connection-oriented transport protocol that provides reliable transport of data between pairs of process. The reliability is ensured by the implementation of flow control and error correction in the protocol.

The flow control between sender and receiver is managed by using sliding windows, window size adjustment heuristics and congestion avoidance algorithms. These three mechanisms should ensure that the resources of a share media are distributed equally among the different sessions in progress.

The acknowledgement sent for each packet that was correctly received constitutes the error correction (control) mechanism in TCP that controls the re-transmission of packets.TCP is suitable for applications that require reliable ransport of data (such as http, ftp, smtp etc).

UDP (User Datagram Protocol)

UDP (User Datagram Protocol) is another transport layer protocol that provides best-effort service for transport of datagram. The service is unreliable and implies no protection from duplication of packets or packet loss. No flow control or error correction is implemented in UDP. The only mechanism that UDP supports to verify if data is corrupted or nor, is a checksum of the payload. If the receiver discovers a corrupted frame by its non-correct checksum, it simply drops the packet without any attempt to ask for re-transmission.

UDP is suitable for some types of RTA (Real Time Applications) where the speed of the transfer is of greater importance than the reliability of the service.

Characteristics	UDP	TCP
QoS	Best effort, not reliable	Reliable service
Protocol Connection	Connection-less	Connection oriented
Acknowledgements	No acknowledgements	All data is acknowledged
Retransmissions	Not implemented	Lost data is automatically retransmitted.
Flow Control	None	Sliding windows; window size adjustment, congestion avoidance
Overhead	Very low	Low, but higher than UDP
Transmission Speed	Very high	High, but not as high as UDP
Suitable for:	1. When speed is a priority more than reliability. 2. Transfer of small data packets 3. Where multicast/broadcast are used	Most protocols

Table 4.1: A comparison between the characteristics of UDP and TCP.

Anomalies between TCP and IEEE 802.11 MAC

It is important to mention that TCP does not perform well in IEEE 802.11 wireless networks and multiple researches have been done to enhance its performance.

- IEEE 802.11b MAC known as CSMA/CA channel access method guarantees an equal long term channel access probability to all hosts. The implication is that when one host captures the channel for a long time because its bit rate is low, it penalizes other hosts that use the higher rate.
- TCP assumes that packet lost is due to congestions. TCP cannot distinguish between corruption and congestion, so it unnecessarily reduces window, resulting in low throughput and high latency.

Due to the CSMA/CA protocol overhead, in practice the maximum 802.11b throughput that an application can achieve (in a P to P link) is about 5.9 Mbit/s over TCP and 7.1 Mbit/s over UDP.

It is highly recommended to design to wireless networks as symmetric as possible. Try to get nodes to listen to each other and use similar effective power rates. Include some traffic shaping mechanism in the back bone. Traffic shaping allows controlling TCP congestion and can help to distribute the bandwidth resources evenly.

Layer 3 Firewalls

In the transport layer, a firewall is implemented to control the network traffic by blocking TCP or UDP ports. Since many applications use “well known” ports for their communications, packet filtering can be used to block those port, for example FTP (port 20) or Telnet (port 23) or SMTP (port 25).

There are two different strategies when it comes to firewalls on TCP level. Either we block all ports or only open the ones that we truly need, or we open all ports and then block only the ones that we see as a threat. The more restrictive alternative that blocks all ports that we don’t want to keep open is of course the safest one.

Firewalls use a combination of three main methods:

- block outgoing traffic of type X
- block incoming traffic of type Y
- forwarding traffic of type Z

Forwarding implies that the firewall passes all incoming connection for a certain port to another host and port within the network. By forwarding ports we are creating a pass through in our firewall since we allow incoming packets to enter our network. The main purposes of port forwarding are to provide an external service from an internal firewalled host to provide multiple instances of a service from internal firewalled hosts for the purpose of load balancing.

Firewall design

The firewall is a fundamental part of a wireless network. It can block malicious code entering the wireless network and help us to allow us to decide which services we want to make available to our users. A wireless network should be considered as a "limited" resource and hence needs service prioritization.

A good wireless design should combine a **firewall, traffic shaping and monitoring.** Most of the troubleshooting in wireless networks comes from (1) detecting, (2) blocking and (3) removing malicious programs that exhaust the bandwidth resources.

For example, if we find the use of peer-to-peer programs, a set of limited bandwidth resources should be allocated to them.

Application layer

The main responsibility for the application layer is to ensure that effective communication with other application programs in a network is possible. It is important to understand that the application layer is NOT the application itself. It is purely a service layer that provides the following services:

- Identify and make sure that the other part is ready for communication
- Authenticate (message, sender, receiver)
- Identify necessary communication resources
- Ensure agreement between sender and receiver regarding error recovery procedures, data integrity, privacy
- Determine protocol and data syntax rules at application level.

The most widely used application layer protocols today are HTTPS, SMTP, IMAP/POP3, FTP, Messaging Protocols and RTP on communication through internet.

Application firewalls

The firewall that has been discussed so far has been operating on network and transport layer. With such firewalls, we are able to do the following:

- block or allow incoming traffic from a particular IP address
- block or allow outgoing traffic to a particular IP address
- block or allow incoming/outgoing traffic using a particular TCP or UDP port

What these firewalls can't do is to examine the actual content of that data and block packets based on its contents. For achieving that, we need to filter the data on application layer: Application Layer Filter (ALF).

ALF can identify abnormal information in the header of the message and in the data itself.

It can be configured to search for certain strings in the data to block the message based on that information. With those characteristics, ALF can prevent the following:

- SMTP, POP3 and DNS buffer overflows
- Web server attacks based on information in HTTP headers and requests
- Attack code hidden within SSL tunnels
- Block applications running at the top of HTTP (Messengering)
- Internal users to spread "sensitive: information
- ALF can also block specific commands within the application layer protocols. For example, in HTTP the command GET can be blocked while POST is still allowed.

The primary disadvantage of ALF is its negative effect on performance due to the examination of all data. It also raises some ethical questions as building ALF implies having the capabilities of analyzing personal data in real time.

An implication of that is that more powerful hardware is needed than for traditional packet filtering firewalls which has a direct impact in service level and its price.

A disadvantage that occurs due to the complexity that ALF brings to the network is the risk of wrong configuration of the filter which may result in incorrect blocking of data. So proper tunning is necessary to use such type of devices.

Application Layer Filter

A common variation of application layer filters is anti-virus and anti-spam systems. Anti-virus/spam system is able to examine the contents of the application and block or tag suspicious e-mail attachments.

When designing a wireless network we will have to consider implementing such application layer filter. SPAM consume 30-50% of the total mail traffic. By tagging SPAM and training users to run filter software in their mail clients, we can avoid the transfer of unsolicited mail over wireless links.

Another application layer filter that we might consider implementing is a web proxy server. A web proxy server is used to cache frequently requested data on its memory.

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 include 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	Masking of network
Gateway	IP address of the outgoing connection of your network.
DNS	IP address of the DNS server we announce by DHCP to the wireless clients

Table 4.1: IP related settings of an access point.

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 we change immediately to a stronger password.

Avoid passwords that can be connected with we 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 we 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.

Network topologies and its infrastructure

We have already discussed about the wireless link, link budgeting, and basic networking. Now we are going to discuss about the different kind of network topologies commonly used in networking. This unit considers the physical shape and the logical lawet of basic network topologies in general and wireless topologies in specific. A set of common topologies will be presented and their respective relevance in wireless implementations will be discussed.

Basic network topologies

A network topology is the lawet of connecting links between nodes in a network. Networks can take many different forms depending on how nodes are interconnected. There are two ways of describing the topology of a network:

physically or logically. The physical topology refers to the configuration of cables, computers and other network devices while the logical topology refers to higher abstract level, for example by considering the method and flow of information transfer between nodes.

Below follows a brief description of a set of basic network topologies.

Topology	Description
Bus	All nodes are connected to a shared/common cable. Ethernet networks are normally bus topologies.
Star	Each node is connected directly to a central network hub or concentrator. All data in a star topology passes though the hub before reaching its destination. This topology is common in Ethernet and Wireless LAN.
Line (or multi-hop)	A set of nodes connected in a line. Each node is connected to its two neighbouring nodes except for the end nodes that have only one neighbouring node each.
Tree	A combination of a bus and a star topology. A set of star configured nodes are connected to a bus backbone.
Ring	All nodes are connected to one another in the shape of a closed loop, so that each node is connected directly to two other devices. Typically backbone infrastructure with optical fibre.
Full mesh	A direct link between all pairs of nodes. A full mesh with n nodes requires n(n-1)/2 direct links. Due to its character, it is an expensive topology but very reliable. Mainly used within military applications.
Partial mesh	Some nodes are organized in a full mesh scheme while others are just connected to one or two nodes in the network. Partial mesh topology is less expensive than full mesh but are of course not as reliable since the number redundant links are reduced.

Table 4.2: Description of basic network topologies

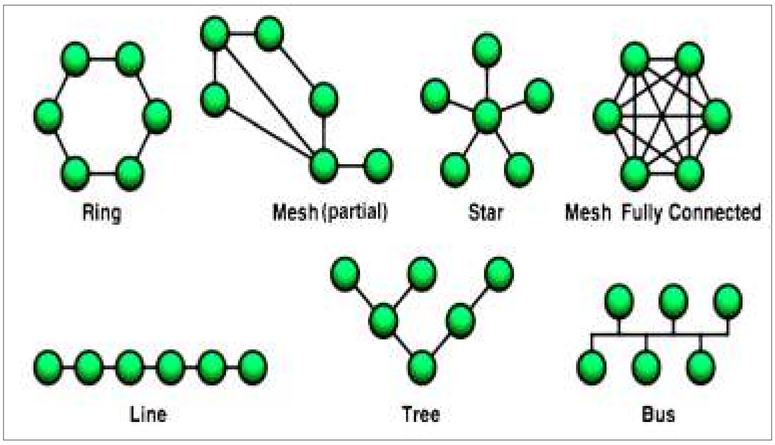


Figure4.11: Basic network topologies

Relevant network topologies in wireless networking

Above some network topologies can or can not be applied to wireless networking. These remarks might sound trivial, but their understanding is elementary for successful wireless networking.

Wireless communication needs no medium

Wireless communication obviously needs no cables or no other medium like: air, ether or other carrier substance. In wireless networking, a line drawn in a network diagram is equivalent to a (potential) connection that is being made, i.e. it is not to a cable or another physical representation.

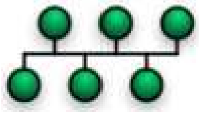
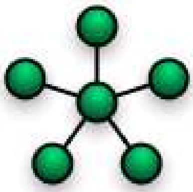
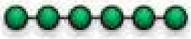
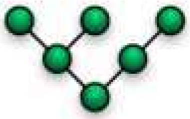
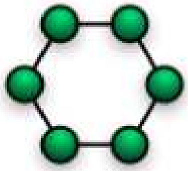
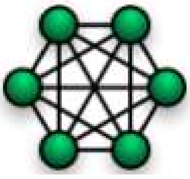
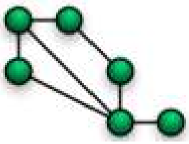
Wireless communication is always two-way (bidirectional)

This bi-directionality exists regardless if we talk about *transmitters* or *receivers*, *masters* or *slave*, *AP* or *CPE*

A radio is a radio and its further role is determined by software

Software determines the radio cards' behavior down to OSI Layer 1 and 2, i.e. the physical and link layer.

With these general remarks in mind, we can evaluate the relevance of network topologies for wireless networking.

Topology	**Visual representation**	**Wireless relevancy**
Bus		Not applicable. Studying the bus topology we will notice that each node is connected to all other nodes and since the place where one line meets the other lines is of no significance in the wireless case, this topology is fully equivalent to a (full) mesh network operating in one single channel.
Star		Yes , the standard topology of wireless network.
Line (multi-hop)		Yes, with two or more elements. A line of two nodes is a PtP link.
Tree		Yes, typically wireless ISPs.
Ring		Yes, possible but rarely found
Full mesh		Yes, but mostly partial mesh
Partial mesh		Yes.

Tabe 4.3: Topologies in wireless networks

Wireless Components

Access point

An access point is a wireless "hub". The transmitter/receiver connects together the wireless nodes and typically also bridges them to the wired network. A set of (coordinated) access points can be connected together to create a large wireless network.

From wireless clients' point of view (laptops or mobile stations), an access point provides a virtual cable between the associated clients.

An access point should be distinguished from a wireless router. A wireless router is a combination of an access point and a router and can perform routing tasks than an Access Point. Consider a wireless router as a wireless bridge (between wireless and wired Ethernet) and a router (IP routing features).

Clients connect to the access points by knowing their "identification". This way of identification is known as the Service Set Identity (SSID) and it should be shared by all members of the specific wireless network. All the wireless clients and access Points within an Extended Service Set (ESS) must be configured with the same ID (ESSID).

When talking about SSID is like "label of an Ethernet socket". Connecting to a wireless network with SSID "x" is equivalent to plugging your computer to Ethernet socket on the wall identified with the tag "x".

Wireless clients

A wireless client is any wireless station that connects to a wireless Local Area Network (LAN) to share its resources. A wireless station is defined as any computer with an installed wireless network adapter card that transmits and receives Radio Frequency (RF) signals.

Some common wireless clients are laptops, PDA's, surveillance equipment and wireless VoIP phones.

Wireless modes

There are two fundamental wireless modes defined in the 802.11 suite of standards:

- Ad Hoc
- Infrastructure

It is important to understand that these modes are not always directly reflected in the topology. For example, a point to point link can be in ad hoc or infrastructure mode and one could imagine a star built out of ad hoc connections.

The mode can be seen as a basic setting of the individual radio card of a node rather than a characteristic of the whole infrastructure.

Ad hoc Mode (IBSS)

The Latin word 'ad hoc' means "for this purpose" but are commonly used for an improvised and often impromptu events or solutions.

Ad hoc mode, also known as Peer-to-Peer, is a method for wireless clients to directly communicating with each other. By allowing wireless clients to operate in ad-hoc mode, there is no need of involving any central Access Points. All nodes of an ad hoc network can communicate directly with the other clients.

Each wireless client in an ad hoc network must be set its wireless adapter in ad hoc mode and use the same SSID and "channel number/frequency".

An ad-hoc network consists normally of a small group of devices located close to each other. Performance decreases as the number of nodes in the ad hoc network grows. In order to bridge an ad hoc network to a wired LAN or to the Internet, a special gateway must be installed.

Independent Basic Service Set (IBSS) is the denotation of the ad hoc mode in IEEE 802.11 networks.

Case 1: Point to Point

Ad hoc mode can be used when we need to connect two stations directly for short period of time e.g. client to client. It can also be used inside of an office between a set of workstations.

Setting	**Node 1**	**Node 2**
Mode	ad hoc	ad hoc
SSID	MY_SSID	MY_SSID
Channel	Need to agree and know each others	Need to agree and know each others
IP address	Typically fixed	Typically fixed

Table 4.4:A typical setup for an ad hoc network.

If one node is networked (e.g. Internet or intranet), it has control to share that network to the other node.

Infrastructure (BSS)

In infrastructure mode there is a "coordination" element: an access point or base station. If the access point is connected to the wired Ethernet network, the wireless clients can access the fixed network via the access point.

When several access points and wireless clients are interconnected, they must be configured to use the same SSID. If we want to ensure that the overall capacity of your network is maximized do not configure all the access points in the same physical area to use the same channel. The clients will discover (by means of scanning) which channel the access point is using and hence, there is no need for the clients to know the channel number in advance.
Basic Service Set (BSS) is the denotation of the infrastructure mode in IEEE 802.11 networks.

Case 1: Star

The star topology is by far the most common infrastructure for wireless networks. It is the typical topology for ahotspot, whether it is in a airport or a Telecenter. The star topology is the typical WISP setup (think in a point to multipoint link). This type of network is often extended into trees or combination with other topology elements.

Setting	AP/Gateway	Node x1
Mode	Infrastructure	Infrastructure
SSID	Sets MY_SSID	Connects to MY_SSID
Channel	Sets channel x	Discovers the channel
IP address	Typically runs DHCP server (if router features are available)	Typically gets IP via DHCP lease

Table 4.5: A typical setup for a star topology

Case 2: Point to Point (PtP)

Point to point (PtP) links is a standard element of a wireless infrastructure. On topology level they may be part of a star topology, a simple 2-point line or other topology. The mode of a PtP link can be ad hoc or infrastructure.

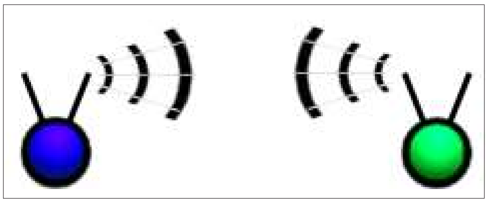


Figure 4.13:A point-to-point link in ad hoc or infrastructure mode.

Setting	Node 1	Node 2
Mode	Any	Any
SSID	MY_SSID	MY_SSID
Channel	Will agree and know each others	Will agree and know each others
IP address	Typically fixed	Typically fixed
MAC address	Might be fixed to one another's MAC	Might be fixed to one another's MAC

Table 4.6: settings of two node for a Ad-hoc mode

A typical setup for a PtP link. The mode can be ad hoc or infrastructure but both nodes must be in the same mode.

For long distance PtP links advanced wireless settings are required to improve performance.

Case 3: Repeating

Repeating typically becomes necessary when the direct line of sight is obstructed or the distance is too long for one single link. The wired equivalent of wireless repeating is a hub.

The setup of repeating depends on hardware and software specific factors and is difficult to describe in one generic way.

The repeating unit may consist of one or two physical devices and have one or two radios. A repeater can also be seen as a receiving client and a re-transmitting access point. Typically, the SSID would be the same for all 3 units.

Often the repeater ties to a MAC Address in addition to a SSID.

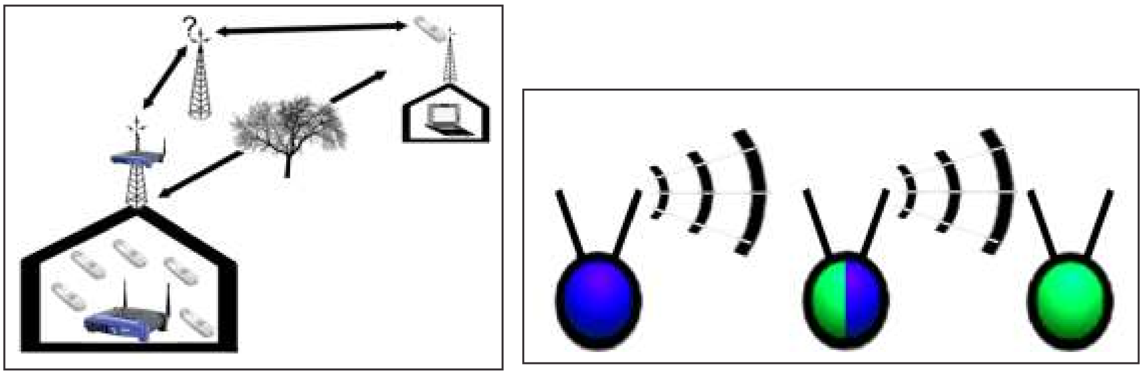


figure 4.14: Two examples of repeating wireless infrastructure.

Case 4: Mesh

Mesh topologies are an interesting option mainly in urban environment but also in remote areas whenever central infrastructure is hard to implement. Typical cases are municipal networks, campus networks and neighborhood communities.

A mesh network is a network that employs one of two connection arrangements, full mesh topology or partial mesh topology. In the full mesh topology, each node is connected directly to each of the others. In the partial mesh topology, nodes are connected to only some, not all, of the other nodes.

Note that this definition mentions no dependency on any time parameter so nothing is necessarily dynamic in a mesh. However, in recent years and in connection with wireless networks, the term "mesh" is often used as a synonym for "ad hoc" or "mobile" network.

All mesh nodes need to run the same mesh routing software (protocol), but can be of different operating systems, and hardware types.

The setup of a mesh network is dependent on the mesh routing protocol and implementation. The table below shows some typical parameters.

Setting	Node x1	Node x2
Mode	ad hoc	ad hoc
SSID	MY_SSID	MY_SSID
Channel	Channel x	Channel x
IP address	Typically static and manually set	Typically static and manually set
MAC address	Might be fixed to one another's MAC	Might be fixed to one another's MAC

Table 4.7: A typical setup for a mesh network.

Using DHCP in mesh networks make difficult to manage, so static IP addresses are recommended. The gateway nodes typically need additional settings to announce their presence.

Real life examples of wireless infrastructures

Real life wireless networks are very often combinations of different topologies. Here are a few examples for discussion.

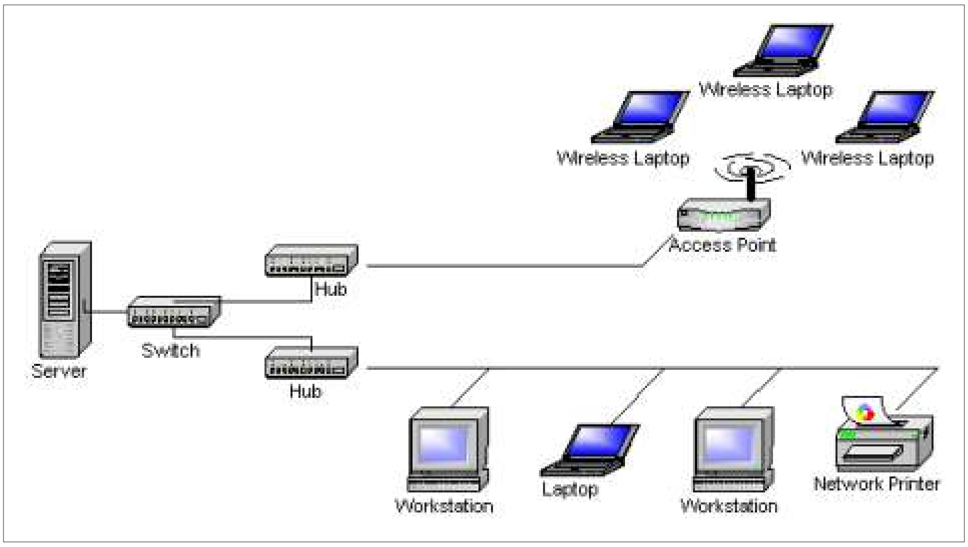


Figure 4.15: A typical office network with wireless part

Radio Device configuration

This unit provides a general methodology for installing and configuring wireless access points. 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 for simplicity, we follow the OSI model with main focus on the physical and the link layer.

Before We Start

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

- Read the manual of the access point and get to know the device and its default settings.
- Consider the physical installation placement (access to power, antennas, temperature, humidity etc.).
- Plan the network (TCP/IP) before we start and make a drawing of the topology. Planning includes knowing your ISP's or LAN settings including DNS, etc.
- Make sure that we have all documentation and material (physically, not only online), so we can work even if we are disconnected during the process.
- Take notes about every step we take in the configuration process, especially when changing IP addresses, network

settings and passwords.

- Make sure that we have all necessary hardware needed (PC/laptop with wireless and Ethernet interfaces)
- Make sure that we 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) .

Installing hardware

The first step of the configuration process is to install the hardware as provided in the manual that comes with device, connect the access point to your computer. This section gives we an overview of the general physical lawet of an access points and how to physically install the device.

Physical installation

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

- Status LEDs (diodes)
- 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 the following parameters with flashing or steady (green or red) light:

- Power to the access point
- Active ports
- Internal error
- Ethernet connection (uplink)

The LEDs can give we highly valuable information while troubleshooting your network. We strongly suggest we 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.

- 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.
- 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.

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

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.

Connect your computer to the device

To configure the access point, we 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 we feel more confident with the configuration process, switch to wireless.

The wired connection can be done using:

- Ethernet cable via HTTP or using vendor specific software based on SNMP (eg. winbox for MikroTik)
- Serial cable (Null modem) using HyperTerminal or other serial communication program (if the access point has a Serial Port)

Among the two 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 we 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, we 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 point configuration which we install on your computer in order to setup a wireless device. They are normally based on a protocol known as SNMP.

Using a serial cable, can be considered as your "backup plan" when things have gone wrong. This option implies that we 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 we have forgotten the password and do not want to reset to default settings. Normally, we can access the access point via the serial interface without knowing the password (or we can set up a non-password via the Serial Cable).

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" access point only needs two settings:

- SSID name
- Channel number

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

Below follows a theoretical approach to hardware configuration that follows the OSI model and puts emphasis 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.

The Physical Layer

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

Channel Number

When setting the channel of an access point, we determine the range of frequencies (GHz) that the device will operate in. Before we set the channel, we 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, we 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 we 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.

Transmit power

The higher the transmit power is, the larger coverage range the access point will give we. If we aim to archive a large coverage, 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 we 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 we use.

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

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 we are building a very long link and experience problems with packet loss, we can try to reduce the speed in order to have a more robust signal.

The Link layer

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

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.

We 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 whether the access point performs bridging or routing/NATing.

The section below describes a set of typical “modes'” that we 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 a 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".

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. The SSID is a case sensitive text string that accepts up to 32 alphanumeric characters and it is used 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"

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, we can monitor and capture certain packets of the wireless network and in that way find the SSID.

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 we sufficient support in terms of mobility within an office environment. If we need support for higher mobility, we 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 we not to change this value unless we have very good reasons to do so.

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

RTS/CTS is a method used by IEEE 802.11 wireless networks to reduce collisions caused by "hidden nodes". 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 follow:

A node that wants to send data initiates the handshake with the access point by sending a RTS frame. The access point 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 are 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, we 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.

Access Control through MAC filtering

MAC filtering implies that we 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 are coming from/to the network and find out which MAC addresses that are granted access. Thereafter, it can change its own MAC address to one of the accepted ones and "fool" the access point by pretending to be someone else.

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 in the access point must always be reflected in the client side. Make sure that your client device supports the encryption protocol, authentication type and key length that we configure your access point to run.

If we choose to enable WEP, always remove the default WEP keys that are provided by the vendor and set your own private keys. If we use 64-bit key (40 bit as actual key) we 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, we 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 need firmware upgrade:

- Wireless access points
- Wireless network adapters
- Wireless client programs (drivers, management tools etc)

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 allowing 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.

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 enables VPN Pass-through via PPTP/IPSec.

Securing Wireless Network

The network is the entry point to your application. It provides the first gatekeepers that control access to the various servers in your environment. Servers are protected with their own operating system gatekeepers, but it is important not to allow them to be deluged with attacks from the network layer. It is equally important to ensure that network gatekeepers cannot be replaced or reconfigured by imposters. In a nutshell, network security involves protecting network devices and the data that they forward.

The basic components of a network, which act as the front-line gatekeepers, are the router, the firewall, and the switch. Figure below shows these core components.

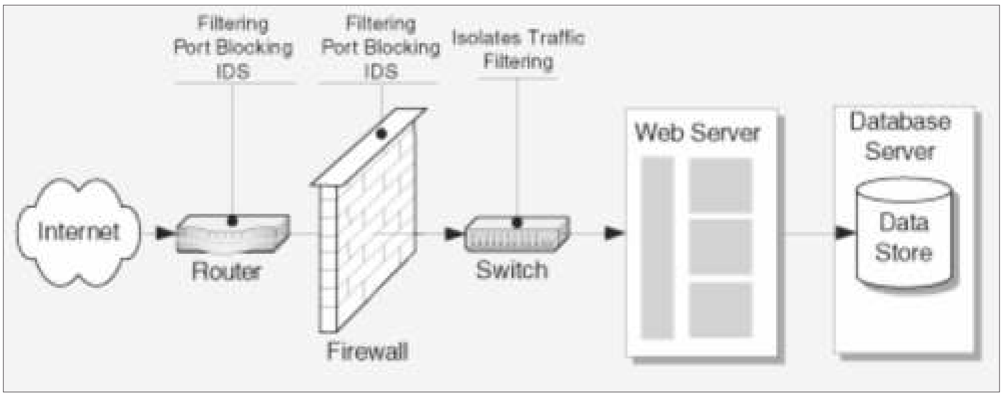


Figure4.18: Network components: router, firewall, and switch

Threats and Countermeasures

An attacker looks for poorly configured network devices to exploit. Common vulnerabilities include weak default installation settings, wide-open access controls, and unpatched devices. The following are high-level network threats:

- Information gathering
- Sniffing
- Spoofing
- Session hijacking
- Denial of service

With knowledge of the threats that can affect the network, we can apply effective countermeasures.

Information Gathering

Information gathering can reveal detailed information about network topology, system configuration, and network devices. An attacker uses this information to mount pointed attacks at the discovered vulnerabilities.

- Vulnerabilities
- Common vulnerabilities that make your network susceptible to an attack include:
- The inherently insecure nature of the TCP/IP protocol suite
- Configuration information provided by banners
- Exposed services that should be blocked
- Attacks
- Common information-gathering attacks include:
- Using Tracert to detect network topology
- Using Telnet to open ports for banner grabbing
- Using port scans to detect open ports
- Using broadcast requests to enumerate hosts on a subnet
- Countermeasures
- We can employ the following countermeasures:
- Use generic service banners that do not give away configuration information such as software versions or names.
- Use firewalls to mask services that should not be publicly exposed.

Sniffing

Sniffing, also called ***eavesdropping,*** is the act of monitoring network traffic for data, such as clear-text passwords or configuration information. With a simple packet sniffer, all plaintext traffic can be read easily. Also, lightweight hashing algorithms can be cracked and the payload that was thought to be safe can be deciphered.

Vulnerabilities

Common vulnerabilities that make your network susceptible to data sniffing include:

- Weak physical security
- Lack of encryption when sending sensitive data
- Services that communicate in plain text or weak encryption or hashing
- Attacks
- The attacker places packet sniffing tools on the network to capture all traffic.
- Countermeasures
- Countermeasures include the following:
- Strong physical security that prevents rogue devices from being placed on the network
- Encrypted credentials and application traffic over the network

Spoofing

Spoofing, also called ***identity obfuscation,*** is a means to hide one's true identity on the network. A fake source address is used that does not represent the actual packet originator's address. Spoofing can be used to hide the original source of an attack or to work around network access control lists (ACLs) that are in place to limit host access based on source address rules.

Vulnerabilities

Common vulnerabilities that make your network susceptible to spoofing include:

- The inherently insecure nature of the TCP/IP protocol suite
- Lack of ingress and egress filtering. Ingress filtering is the filtering of any IP packets with untrusted source addresses before they have a chance to enter and affect your system or network. Egress filtering is the process of filtering outbound traffic from your network.
- Attacks
- An attacker can use several tools to modify outgoing packets so that they appear to originate from an alternate network or host.
- Countermeasures
- We can use ingress and egress filtering on perimeter routers.

Session Hijacking

With session hijacking, also known as man in the middle attacks, the attacker uses an application that masquerades as either the client or the server. This results in either the server or the client being tricked into thinking that the upstream host is the legitimate host. However, the upstream host is actually an attacker's host that is manipulating the network so that it appears to be the desired destination. Session hijacking can be used to obtain logon information that can then be used to gain access to a system or to confidential information.

Vulnerabilities

Common vulnerabilities that make your network susceptible to session hijacking include:

- Weak physical security
- The inherent insecurity of the TCP/IP protocol suite
- Unencrypted communication
- Attacks
- An attacker can use several tools to combine spoofing, routing changes, and packet manipulation.
- Countermeasures
- Countermeasures include the following:
- Session encryption
- Stateful inspection at the firewall

Denial of Service

A denial of service attack is the act of denying legitimate users access to a server or services. Network-layer denial of service attacks usually try to deny service by flooding the network with traffic, which consumes the available bandwidth and resources.

Vulnerabilities

Vulnerabilities that increase the opportunities for denial of service include:

- The inherent insecurity of the TCP/IP protocol suite
- Weak router and switch configuration
- Unencrypted communication
- Service software bugs

Attacks

Common denial of service attacks include:

- Brute force packet floods, such as cascading broadcast attacks
- SYN flood attacks
- Service exploits, such as buffer overflows
- Countermeasures
- Countermeasures include:
- Filtering broadcast requests
- Filtering Internet Control Message Protocol (ICMP) requests
- Patching and updating of service software

Methodology

Security begins with an understanding of how the system or network that needs to be secured works. This chapter breaks down network security by devices, which allows we to focus on single points of configuration.

In keeping with this guide's philosophy, this chapter uses the approach of analyzing potential threats; without these analyses, it's impossible to properly apply security.

The network infrastructure can be broken into the following three layers: access, distribution, and core. These layers contain all of the hardware necessary to control access to and from internal and external resources. The chapter focuses on the software that drives the network hardware that is responsible for delivering ASP.NET applications. The recommendations apply to an Internet or intranet-facing Web zone and therefore might not apply to your internal or corporate network.

The following are the core network components:

- Router
- Firewall
- Switch

The router is the outermost security gate. It is responsible for forwarding IP packets to the networks to which it is connected. These packets can be inbound requests from Internet clients to your Web server, request responses, or outgoing requests from internal clients. The router should be used to block unauthorized or undesired traffic between networks. The router itself must also be secured against reconfiguration by using secure administration interfaces and ensuring that it has the latest software patches and updates applied.

Firewall

The role of the firewall is to block all unnecessary ports and to allow traffic only from known ports. The firewall must be capable of monitoring incoming requests to prevent known attacks from reaching the Web server. Coupled with intrusion detection, the firewall is a useful tool for preventing attacks and detecting intrusion attempts, or in worst-case scenarios, the source of an attack.

Like the router, the firewall runs on an operating system that must be patched regularly. Its administration interfaces must be secured and unused services must be disabled or removed.

Switch

The switch has a minimal role in a secure network environment. Switches are designed to improve network performance to ease administration. For this reason, we can easily configure a switch by sending specially formatted packets to it.

Router Considerations

The router is the very first line of defense. It provides packet routing, and it can also be configured to block or filter the forwarding of packet types that are known to be vulnerable or used maliciously, such as ICMP or Simple Network Management Protocol (SNMP).

If we don't have control of the router, there is little we can do to protect your network beyond asking your ISP what defense mechanisms they have in place on their routers.

The configuration categories for the router are:

- Patches and updates
- Protocols
- Administrative access
- Services
- Auditing and logging
- Intrusion detection
- Patches and Updates

Subscribe to alert services provided by the manufacturer of your networking hardware so that we can stay current with both security issues and service patches. As vulnerabilities are found — and they inevitably will be found — good vendors make patches available quickly and announce these updates through e-mail or on their Web sites. Always test the updates before implementing them in a production environment.

Protocols

Denial of service attacks often take advantage of protocol-level vulnerabilities, for example, by flooding the network. To counter this type of attack, we should:

- Use ingress and egress filtering.
- Screen ICMP traffic from the internal network.
- Use Ingress and Egress Filtering

Spoofed packets are representative of probes, attacks, and a knowledgeable attacker. Incoming packets with an internal address can indicate an intrusion attempt or probe and should be denied entry to the perimeter network. Likewise, set up your router to route outgoing packets only if they have a valid internal IP address. Verifying outgoing packets does not protect we from a denial of service attack, but it does keep such attacks from originating from your network.

This type of filtering also enables the originator to be easily traced to its true source since the attacker would have to use a valid — and legitimately reachable — source address. For more information, see "Network Ingress Filtering: Defeating Denial of Service Attacks Which Employ IP Source Address Spoofing" at http://www.rfc-editor.org/rfc/rfc2267.txt.

Screen ICMP Traffic from the Internal Network

ICMP is a stateless protocol that sits on top of IP and allows host availability information to be verified from one host to another. Commonly used ICMP messages are shown in Table 15.1.

Message	Description
Echo request	Determines whether an IP node (a host or a router) is available on the network
Echo reply	Replies to an ICMP echo request
Destination unreachable	Informs the host that a datagram cannot be delivered
Source quench	Informs the host to lower the rate at which it sends datagrams because of congestion
Redirect	Informs the host of a preferred route
Time exceeded	Indicates that the time to live (TTL) of an IP datagram has expired

Table 4.7: Commonly Used ICMP Messages

Blocking ICMP traffic at the outer perimeter router protects we from attacks such as cascading ping floods. Other ICMP vulnerabilities exist that justify blocking this protocol. While ICMP can be used for troubleshooting, it can also be used for network discovery and mapping. Therefore, control the use of ICMP. If we must enable it, use it in echo-reply mode only.

Prevent TTL Expired Messages with Values of 1 or 0

Trace routing uses TTL values of 1 and 0 to count routing hops between a client and a server. Trace routing is a means to collect network topology information. By blocking packets of this type, we prevent an attacker from learning details about your network from trace routes.

Do Not Receive or Forward Directed Broadcast Traffic

Directed broadcast traffic can be used to enumerate hosts on a network and as a vehicle for a denial of service attack. For example, by blocking specific source addresses, we prevent malicious echo requests from causing cascading ping floods.

Source addresses that should be filtered are shown in Table 15.2.

Source address	Description
0.0.0.0/8	Historical broadcast
10.0.0.0/8	RFC 1918 private network
127.0.0.0/8	Loopback
169.254.0.0/16	Link local networks
172.16.0.0/12	RFC 1918 private network
192.0.2.0/24	TEST-NET
192.168.0.0/16	RFC 1918 private network
224.0.0.0/4	Class D multicast
240.0.0.0/5	Class E reserved
248.0.0.0/5	Unallocated
255.255.255.255/32	Broadcast

Table 4.8 : Source Addresses That Should be Filtered

For more information on broadcast suppression using Cisco routers, see "Configuring Broadcast Suppression" on the Cisco Web site at
http://www.cisco.com/en/US/prod/collateral/switches/ps5718/ps708/prod_white_paper0900aecd802ca5d6.html.

Administrative Access

From where will the router be accessed for administration purposes? Decide over which interfaces and ports an administration connection is allowed and from which network or host the administration is to be performed. Restrict access to those specific locations. Do not leave an Internet-facing administration interface available without encryption and countermeasures to prevent hijacking. In addition:

- Disable unused interfaces.
- Apply strong password policies.
- Use static routing.
- Audit Web facing administration interfaces.

Disable Unused Interfaces

Only required interfaces should be enabled on the router. An unused interface is not monitored or controlled, and it is probably not updated. This might expose we to **unknown attacks on those interfaces.**

Apply Strong Password Policies

Brute force password software can launch more than just dictionary attacks. It can discover common passwords where a letter is replaced by a number. For example, if "p4ssw0rd" is used as a password, it can be cracked. Always use uppercase and lowercase, number, and symbol combinations when creating passwords.

Use Static Routing

Static routing prevents specially formed packets from changing routing tables on your router. An attacker might try to change routes to cause denial of service or to forward requests to a rogue server. By using static routes, an administrative interface must first be compromised to make routing changes.

Audit Web Facing Administration Interfaces

Also determine whether internal access can be configured. When possible, shut down the external administration interface and use internal access methods with ACLs.

Services

On a deployed router, every open port is associated with a listening service. To reduce the attack surface area, default services that are not required should be shut down. Examples include**bootps** and **Finger,** which are rarely required. We should also scan your router to detect which ports are open.

Auditing and Logging

By default, a router logs all deny actions; this default behavior should not be changed. Also secure log files in a central location. Modern routers have an array of logging features that include the ability to set severities based on the data logged. An auditing schedule should be established to routinely inspect logs for signs of intrusion and probing.

Intrusion Detection

With restrictions in place at the router to prevent TCP/IP attacks, the router should be able to identify when an attack is taking place and notify asystem administrator of the attack.

Attackers learn what your security priorities are and attempt to work around them. Intrusion Detection Systems (IDSs) can show where the perpetrator is attempting attacks.

Firewall Considerations

A firewall should exist anywhere we interact with an untrusted network, especially the Internet. It is also recommended that we separate your Web servers from downstream application and database servers with an internal firewall.

aAfter the router, with its broad filters and gatekeepers, the firewall is the next point of attack. In many (if not most) cases, we do not have administrative access to the upstream router. Many of the filters and ACLs that apply to the router can also be implemented at the firewall. The configuration categories for the firewall include:

- Patches and updates
- Filters
- Auditing and logging
- Perimeter networks
- Intrusion detection

Patches and Updates

Subscribe to alert services provided by the manufacturer of your firewall and operating system to stay current with both security issues and service patches.

Filters

Filtering published ports on a firewall can be an effective and efficient method of blocking malicious packets and payloads. Filters range from simple packet filters that restrict traffic at the network layer based on source and destination IP addresses and port numbers, to complex application filters that inspect application-specific payloads. A defense in depth approach that uses layered filters is a very effective way to block attacks. There are six common types of firewall filters:

Packet filters

These can filter packets based on protocol, source or destination port number and source or destination address, or computer name. IP packet filters are static, and communication through a specific port is either allowed or blocked. Blocked packets are usually logged, and a secure packet filter denies by default.

At the network layer, the payload is unknown and might be dangerous. More intelligent types of filtering must be configured to inspect the payload and make decisions based on access control rules.

Circuit-level filters

These inspect sessions rather than payload data. An inbound or outbound client makes a request directly against the firewall/gateway, and in turn the gateway initiates a connection to the server and acts as a broker between the two connections. With knowledge of application connection rules, circuit level filters ensure valid interactions. They do not inspect the actual payload, but they do count frames to ensure packet integrity and prevent session hijacking and replaying.

Application filters

Smart application filters can analyze a data stream for an application and provide application-specific processing, including inspecting, screening or blocking, redirecting, and even modifying the data as it passes through the firewall. Application filters protect against attacks such as the following:

- Unsafe SMTP commands
- Attacks against internal DNS servers.
- HTTP-based attacks (for example, Code Red and Nimda, which use application-specific knowledge)

For example, an application filter can block an HTTP DELETE, but allow an HTTP GET. The capabilities of content screening, including virus detection, lexical analysis, and site categorization, make application filters very effective in Web scenarios both as security measures and in enforcement of business rules.

Stateful inspection

Application filters are limited to knowledge of the payload of a packet and therefore make filtering decisions based only on the payload. Stateful inspection uses both the payload and its context to determine filtering rules. Using the payload and the packet contents allow stateful inspection rules to ensure session and communication integrity. The inspection of packets, their payload, and sequence limits the scalability of stateful inspection.

Custom application filters

These filters ensure the integrity of application server/client communication.

When we use filters at multiple levels of the network stack, it helps make your environment more secure. For example, a packet filter can be used to block IP traffic destined for any port other than port 80, and an application filter might further restrict traffic based on the nature of the HTTP verb. For example, it might block HTTP DELETE verbs.

Logging and Auditing

Logging all incoming and outgoing requests — regardless of firewall rules — allows we to detect intrusion attempts or, even worse, successful attacks that were previously undetected. Historically, network administrators sometimes had to analyze audit logs to determine how an attack succeeded. In those cases, administrators were able to apply solutions to the vulnerabilities, learn how they were compromised, and discover other vulnerabilities that existed.

- Apply the following policies for logging and log auditing.
- Log all traffic that passes through the firewall.
- Maintain healthy log cycling that allows quick data analysis. The more data we have, the larger the log file size.
- Make sure the firewall clock is synchronized with the other network hardware.
- Perimeter Networks

A firewall should exist anywhere your servers interact with an untrusted network. If your Web servers connect to a back-end network, such as a bank of database servers or corporate network, a screen should exist to isolate the two networks. While the Web zone has the greatest degree of exposure, a compromise in the Web zone should not result in the compromise of downstream networks.

By default, the perimeter network should block all outbound connections except those that are expected.

- Advantages of a Perimeter Network
- The perimeter network provides the following advantages:
- Hosts are not directly exposed to untrusted networks.
- Exposed or published services are the only point of external attack.
- Security rules can be enforced for access between networks.
- Disadvantages of a Perimeter Network
- The disadvantages of a perimeter network include:
- Network complexity
- IP address allocation and management
- Requirement that the application architecture accommodate the perimeter network design

Switch Considerations

A switch is responsible for forwarding packets directly to a host or network segment, rather than sharing the data with the entire network. Therefore, traffic is not shared between switched segments. This is a preventive measure against packet sniffing between networks. An attacker can circumvent this security by reconfiguring switching rules using easily accessed administrative interfaces, including known account names and passwords and SNMP packets.

The following configuration categories are used to ensure secure switch configuration:

- Patches and updates
- Virtual Local Area Networks (VLANs)
- Insecure defaults
- Services
- Encryption
- Patches and Updates
- Patches and updates must be tested and installed as soon as they are available.
- VLANs

Virtual LANs allow we to separate network segments and apply access control based on security rules. However, a VLAN enhances network performance, but doesn't necessarily provide security. Limit the use of VLANs to the perimeter network (behind the firewall) since many insecure interfaces exist for ease of administration. For more information about VLANs, see the article "Configuring VLANS" on the Cisco Web site.

Insecure Defaults

To make sure that insecure defaults are secured, change all factory default passwords and SNMP community strings to prevent network enumeration or total control of the switch. Also investigate and identify potentially undocumented accounts and change the default names and passwords. These types of accounts are often found on well-known switch types and are well publicized and known by attackers.

Services

Make sure that all unused services are disabled. Also make sure that Trivial File Transfer Protocol (TFTP) is disabled, Internet-facing administration points are removed, and ACLs are configured to limit administrative access.

Encryption

Although it is not traditionally implemented at the switch, data encryption over the wire ensures that sniffed packets are useless in cases where a monitor is placed on the same switched segment or where the switch is compromised, allowing sniffing across segments.

Additional Considerations

The following considerations can further improve network security:

Ensure that clocks are synchronized on all network devices. Set the network time and have all sources synchronized to a known, reliable time source.

Use Terminal Access Controller Access Control System (TACACS) or Remote Authentication Dial-In User Service (RADIUS) authentication for highly secure environments as a means of limiting administrative access to the network.

Define an IP network that can be easily secured using ACLs at subnets or network boundaries whenever possible.

Snapshot of a Secure Network

Table shown below provides a snapshot of the characteristics of a secure network. The security settings are abstracted from industry security experts and real-world applications in secure deployments. We can use the snapshot as a reference point when evaluating your own solution.

Component	**Characteristic**
Router	
Patches and Updates	Router operating system is patched with up-to-date software.
Protocols	Unused protocols and ports are blocked. Ingress and egress filtering is implemented. ICMP traffic is screened from the internal network. TTL expired messages with values of 1 or 0 are blocked (route tracing is disabled). Directed broadcast traffic is not forwarded. Large ping packets are screened. Routing Information Protocol (RIP) packets, if used, are blocked at the outermost router.
Administrative access	Unused management interfaces on the router are disabled. A strong administration password policy is enforced. Static routing is used. Web-facing administration is disabled.
Services	Unused services are disabled (for example **bootps** and **Finger**).
Auditing and logging	Logging is enabled for all denied traffic. Logs are centrally stored and secured. Auditing against the logs for unusual patterns is in place.
Intrusion detection Firewall	IDS is in place to identify and notify of an active attack.
Patches and updates	Firewall software and OS are patched with latest security updates.
Filters	Packet filtering policy blocks all but required traffic in both directions. Application-specific filters are in place to restrict unnecessary traffic.
Logging and auditing	All permitted traffic is logged. Denied traffic is logged. Logs are cycled with a frequency that allows quick data analysis. All devices on the network are synchronized to a common time source.
Perimeter networks	Perimeter network is in place if multiple networks require access to servers. Firewall is placed between untrusted networks.

Component	Characteristic
Switch	
Patches and updates	Latest security patches are tested and installed or the threat from known vulnerabilities is mitigated.
VLANs	Make sure VLANs are not overused or overly trusted.
Insecure defaults	All factory passwords are changed. Minimal administrative interfaces are available. Access controls are configured to secure SNMP community strings.
Services	Unused services are disabled.
Encryption	Switched traffic is encrypted.
Other	
Log synchronization	All clocks on devices with logging capabilities are synchronized.
Administrative access to the network	TACACS or RADIUS is used to authenticate administrative users.
Network ACLs	The network is structured so ACLs can be placed on hosts and networks.

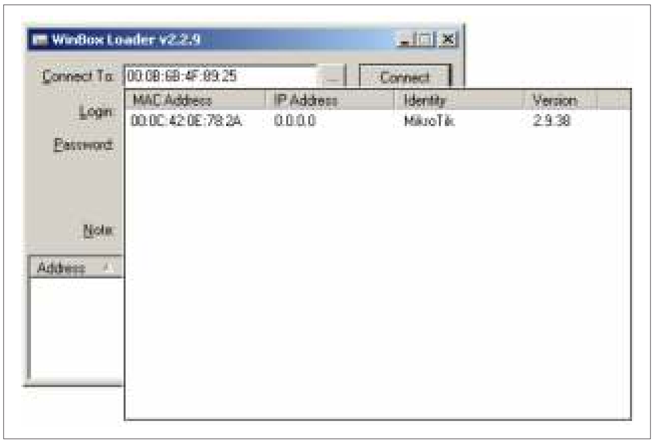
Table4.9: Snapshot of a Secure Network

Example: Access Point Configuration in MikroTik

Start by opening the Wireless Interface window in Winbox. We will see some wireless cards listed here, they might be disabled - to turn them on, click on the blue Enable button. Make sure that the interface is configured and the antennas are connected before we enable an interface.

Accessing the MikroTik AP

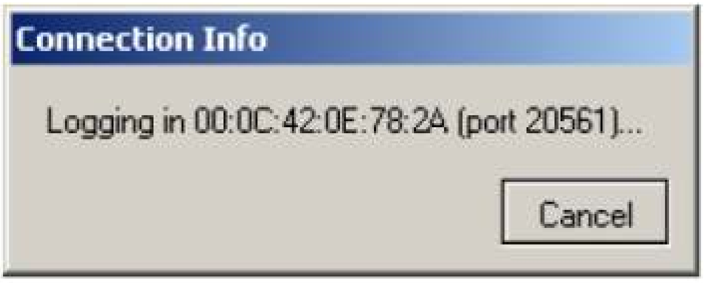
1) Power up your MikroTik AP
2) Connect the AP directly to a PC using a cross over cable, or directly to a hub / switch
3) Run Winbox
4) Click on the '...' button to view connected MikroTik devices



Connect To: 00:0B:6B:4F:89:25

MAC Address	IP Address	Identity	Version
00:0C:42:0E:78:2A	0.0.0.0	MikroTik	2.9.38

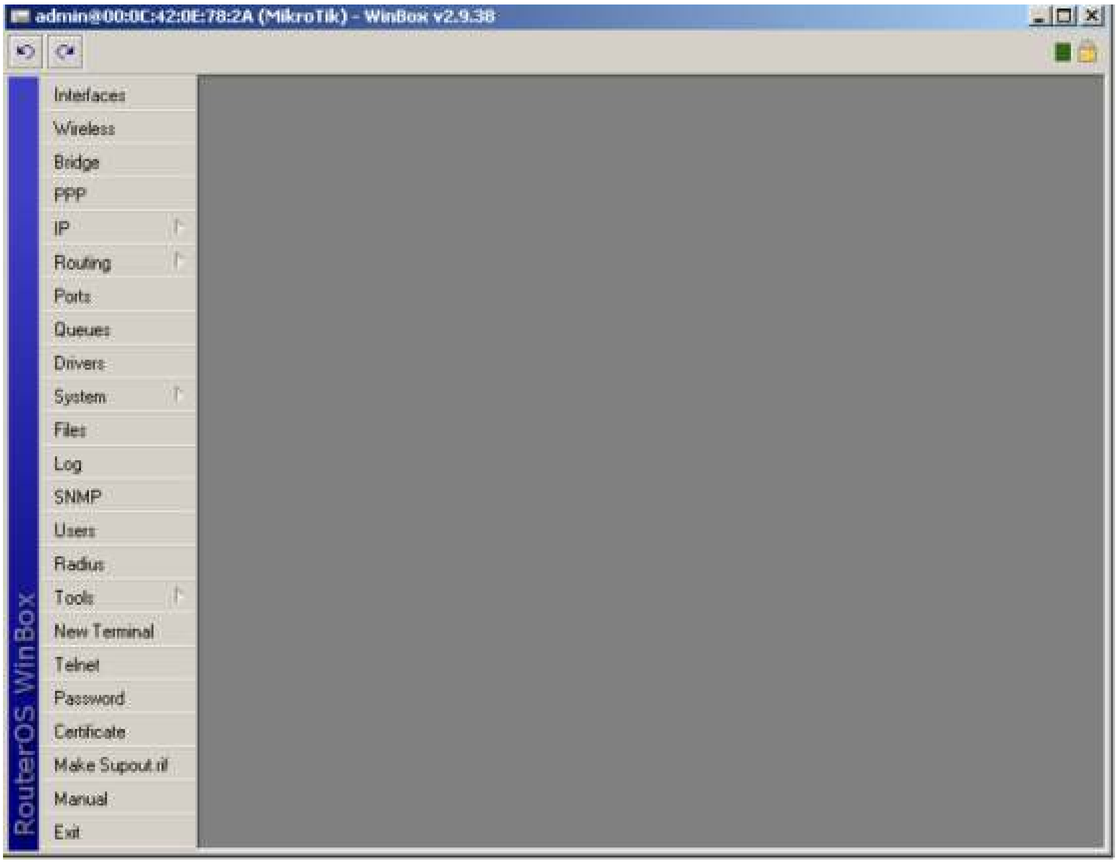
1. Accessing the MikroTik AP
1) Power up your MikroTik AP
2) Connect the AP directly to a PC using a cross over cable, or directly to a hub / switch
3) Run Winbox
4) Click on the '...' button to view connected MikroTik devices
5) Select the device and click on connect



Connection Info

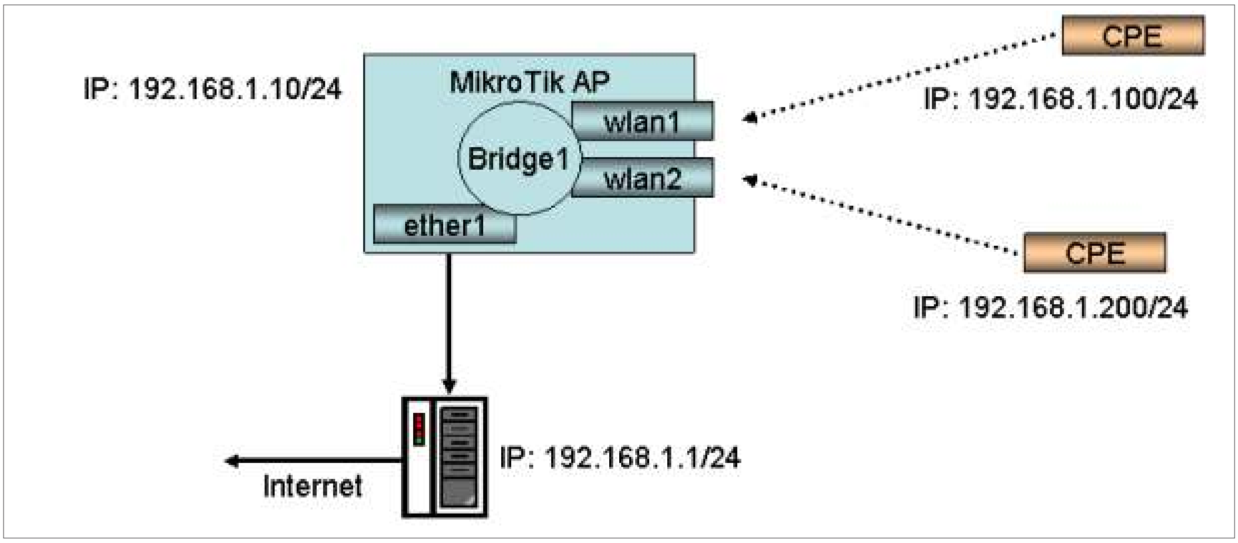
Logging in 00:0C:42:0E:78:2A (port 20561)...

6) You are now connected to your MikroTik AP



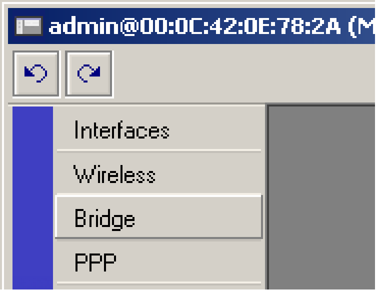
once you have assigned the AP an ip address it can also be accessed using PuTTY.

MikroTik Bridged AP setup

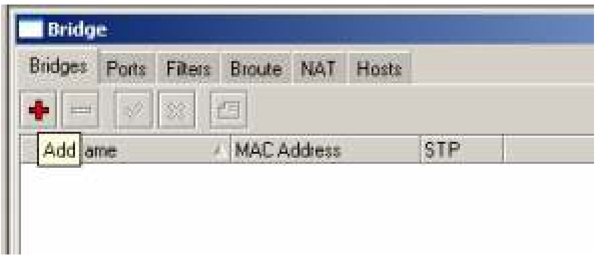


In this, the simplest setup we will create a dual access point (i.e. two radios, both set as an AP) and bridge all the interfaces. The internet is accessed through a server connected to the wired interface.

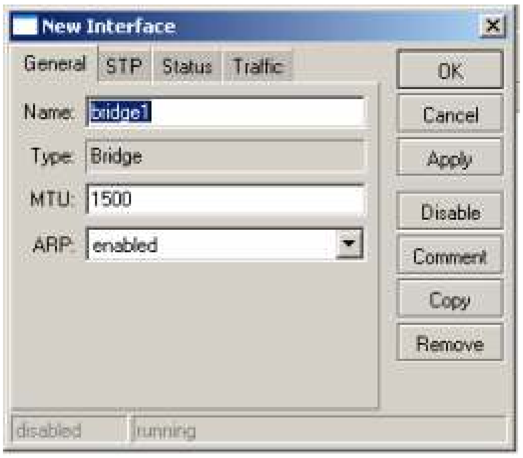
1) Select Bridge



2) Click on the red '+' to add a new bridge



3) Accept all defaults and click on ok



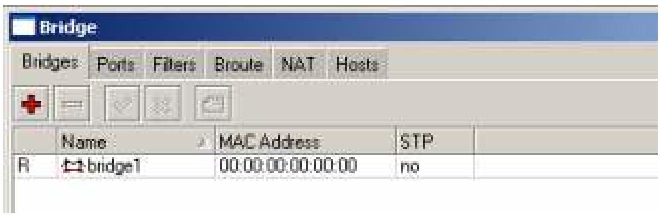
Name: bridge1

Type: Bridge

MTU: 1500

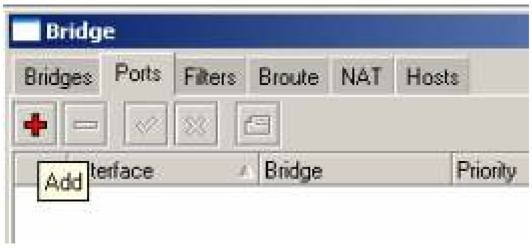
ARP: enabled

4) Click on the Ports tab

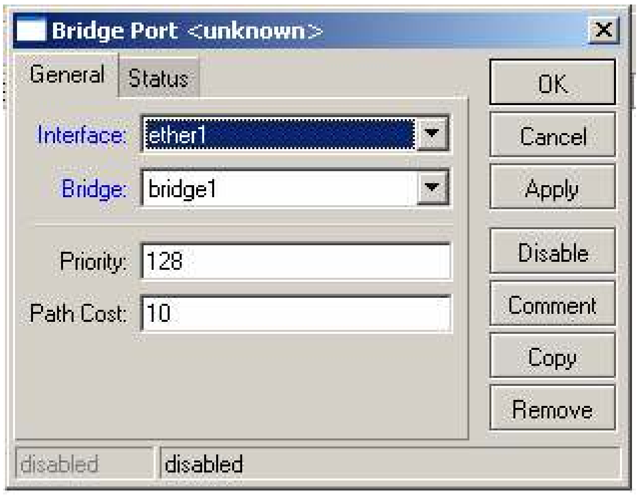


	Name	MAC Address	STP
R	bridge1	00:00:00:00:00:00	no

5) Click on the red '+' to add a new port



6) Select Interface -> ether1, Bridge -> bridge1



Interface: ether1

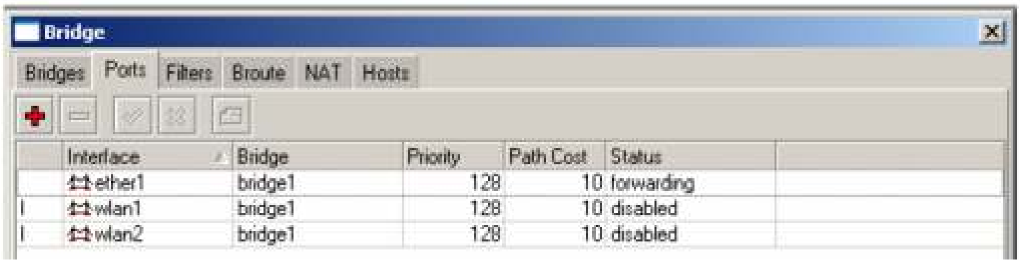
Bridge: bridge1

Priority: 128

Path Cost: 10

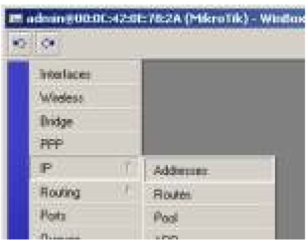
disabled | disabled

7) Click on the red '+' again. This time select Interface -> wlan1, Bridge -> bridge1
8) Click on the red '+' again. This time select Interface -> wlan2, Bridge -> bridge1



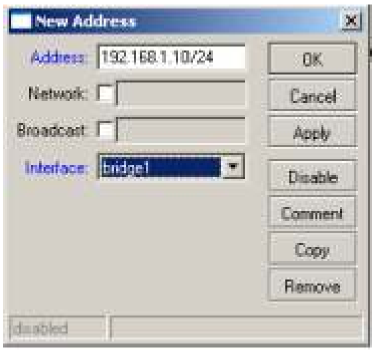
	Interface	Bridge	Priority	Path Cost	Status
	ether1	bridge1	128	10	forwarding
I	wlan1	bridge1	128	10	disabled
I	wlan2	bridge1	128	10	disabled

9) Close the Brige window
10) Click on IP - > Addresses



11) Click on the red'+' to add an address
12) Enter the ip adderss 192.168.1.10/24 in the address field
13) In the interface drop down list box select bridge 1, the click on ok

NOTE All address formats in MikroTik are in address/subnet format, i.e. 192.168..1.1/24. For a more detailed explanation of this notation please see the appendix at the end of this document.



Address: 192.168.1.10/24

Network: □

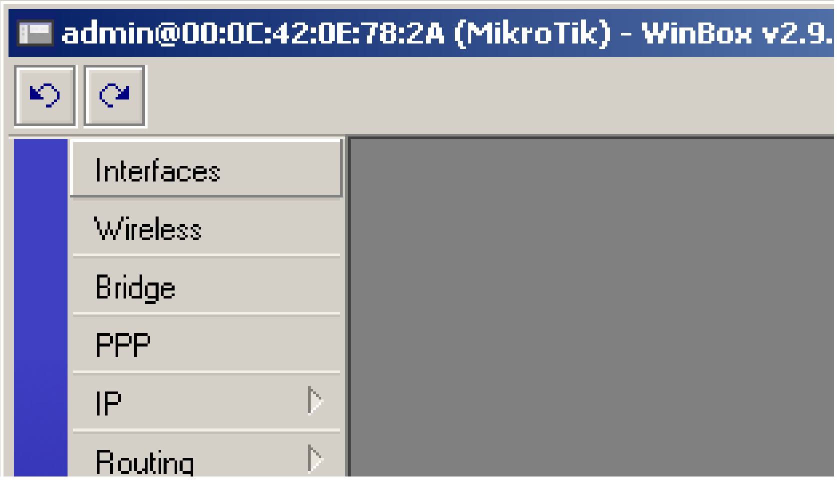
Broadcast: □

Interface: bridge1

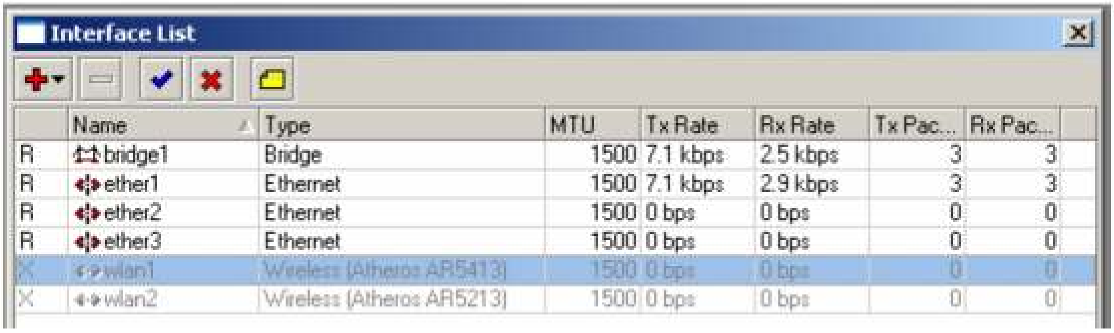
disabled

14) Close the Address List dialog box

15) Select Interfaces

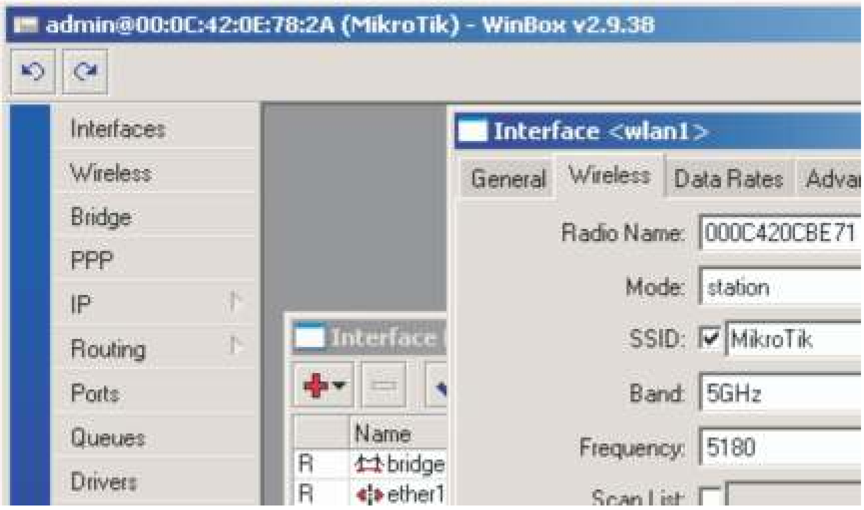

admin@00:0C:42:0E:78:2A (MikroTik) - WinBox v2.9.

16) Double click on wlan1 to configure


Interface List

	Name	Type	MTU	Tx Rate	Rx Rate	Tx Pac...	Rx Pac...
R	bridge1	Bridge	1500	7.1 kbps	2.5 kbps	3	3
R	ether1	Ethernet	1500	7.1 kbps	2.9 kbps	3	3
R	ether2	Ethernet	1500	0 bps	0 bps	0	0
R	ether3	Ethernet	1500	0 bps	0 bps	0	0
X	wlan1	Wireless (Atheros AR5413)	1500	0 bps	0 bps	0	0
X	wlan2	Wireless (Atheros AR5213)	1500	0 bps	0 bps	0	0

17) Click on the wireless tab


admin@00:0C:42:0E:78:2A (MikroTik) - WinBox v2.9.38

Interface <wlan1>

Radio Name: 000C420CBE71

Mode: station

SSID: ☑ MikroTik

Band: 5GHz

Frequency: 5180

Scan List: □

18) In the Mode drop down select ap bridge

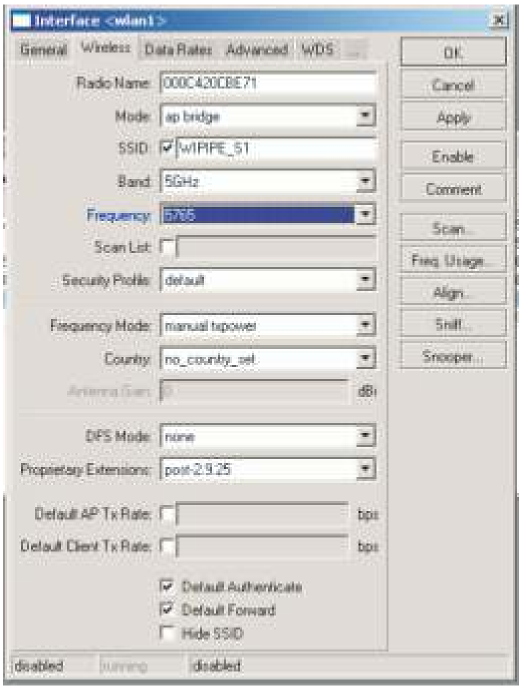
19) Enter the desired SSID in the SSID field

20) In the Band drop down select either 5GHz or 2.4GHz-B

NOTE Wi-Pipe recommends using 802.11b only at 2.4 GHz as this standard has more robust signals

NOTE Wi-Pipe recommends not using the same SSID on multiple AP's as this can cause circular networks. These will cause error's in your network and may prevent you from accessing your AP remotely.

21) In the Frequency field enter the desired frequency
22) Click on ok to save changes



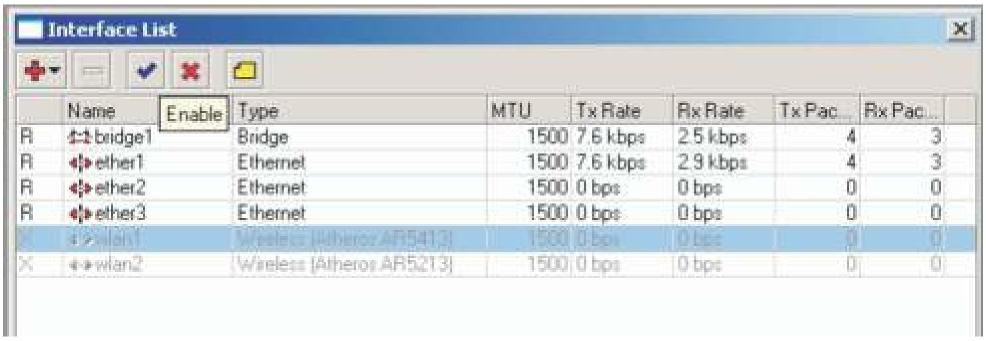
Interface <wlan1>

General | Wireless | Data Rates | Advanced | WDS | ...

Radio Name: 000C420CBE71
Mode: ap bridge
SSID: ☑ WIPIPE_51
Band: 5GHz
Frequency: 5765
Scan List: ☐
Security Profile: default
Frequency Mode: manual txpower
Country: no_country_set
Antenna Gain: 0 dBi
DFS Mode: none
Proprietary Extensions: post-2.9.25
Default AP Tx Rate: ☐ bps
Default Client Tx Rate: ☐ bps
☑ Default Authenticate
☑ Default Forward
☐ Hide SSID

disabled | running | disabled

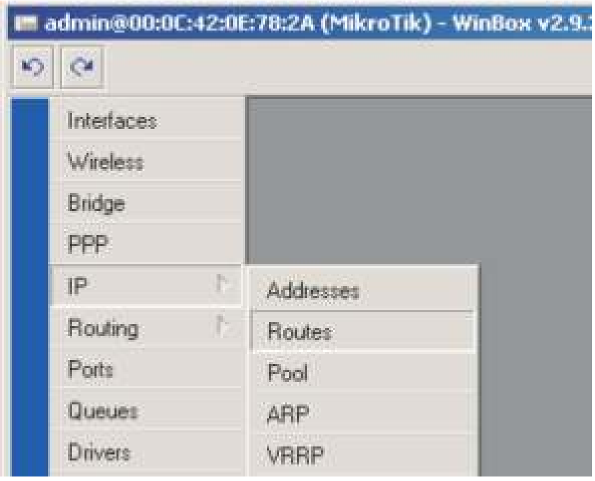
23) Repeat for wlan2 (remember not to use the same SSID on both radio's)
24) Select wlan1 and click on the blue icon to enable the interface



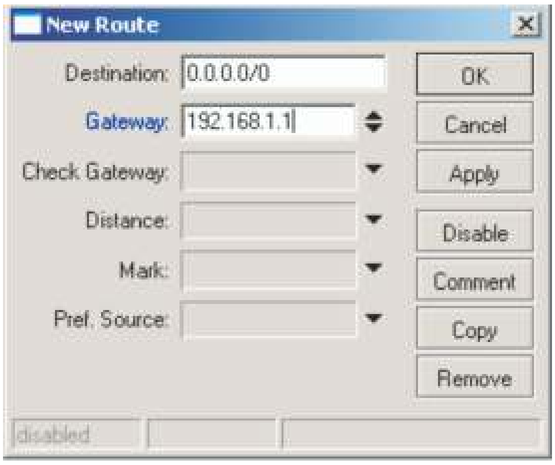
Interface List

	Name	Type	MTU	Tx Rate	Rx Rate	Tx Pac...	Rx Pac...
R	bridge1	Bridge	1500	7.6 kbps	2.5 kbps	4	3
R	ether1	Ethernet	1500	7.6 kbps	2.9 kbps	4	3
R	ether2	Ethernet	1500	0 bps	0 bps	0	0
R	ether3	Ethernet	1500	0 bps	0 bps	0	0
X	wlan1	Wireless (Atheros AR5413)	1500	0 bps	0 bps	0	0
X	wlan2	Wireless (Atheros AR5213)	1500	0 bps	0 bps	0	0

25) Select wlan2 and click on the blue to enable the Interface
26) Close the Interface window
27) Select IP -> Routes

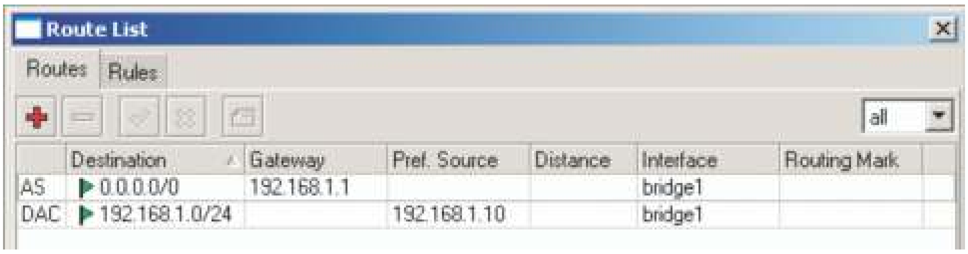


28) Click on the red '+' to add the default route
29) In the destination field enter the address 0.0.0.0/0 (this is the notation for the default route)
30) In the gateway field in the ip address 192.168.1.1



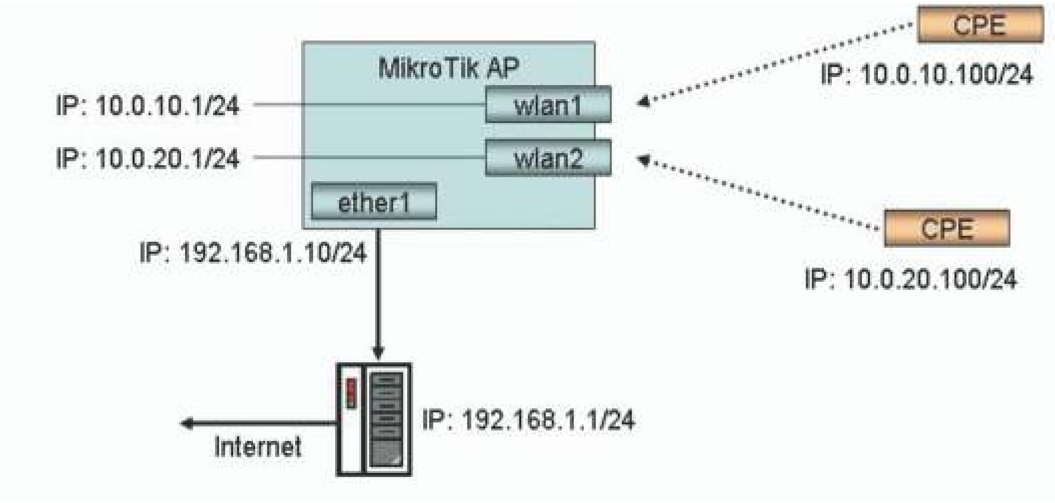
Destination: 0.0.0.0/0
Gateway: 192.168.1.1
Check Gateway:
Distance:
Mark:
Pref. Source:

31) Click on ok to save changes



	Destination	Gateway	Pref. Source	Distance	Interface	Routing Mark
AS	▶ 0.0.0.0/0	192.168.1.1			bridge1	
DAC	▶ 192.168.1.0/24		192.168.1.10		bridge1	

2. MikroTik Routed Setup

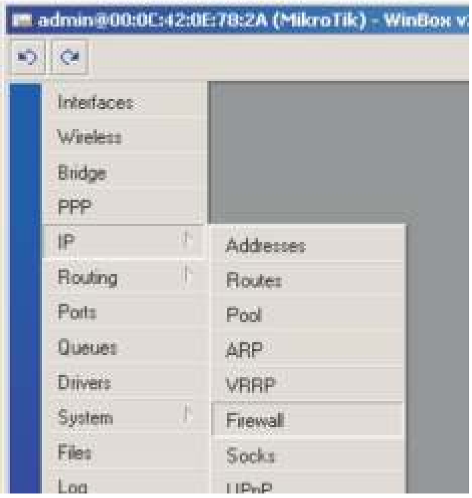


This guide highlights the differences between a bridged and a routed setup. Note this assumes you have not created the bridge and have not yet assigned an ip address to any interface.

1) Click on IP -> Address
2) Click on the red '+' to add an address
3) Enter the ip address 192.168.1.10/24, Interface -> ether1
4) Click on the red '+' to add another address
5) Enter the ip address 10.0.10.1/24, Interface -> wlan1
6) Click on the red '+' to add another address

7) Enter the ip address 10.0.20.1/24, Interface -> wlan2

8) Click on IP -> Routes and add 192.168.1.1 as the default route as per steps 27 to 31 above.

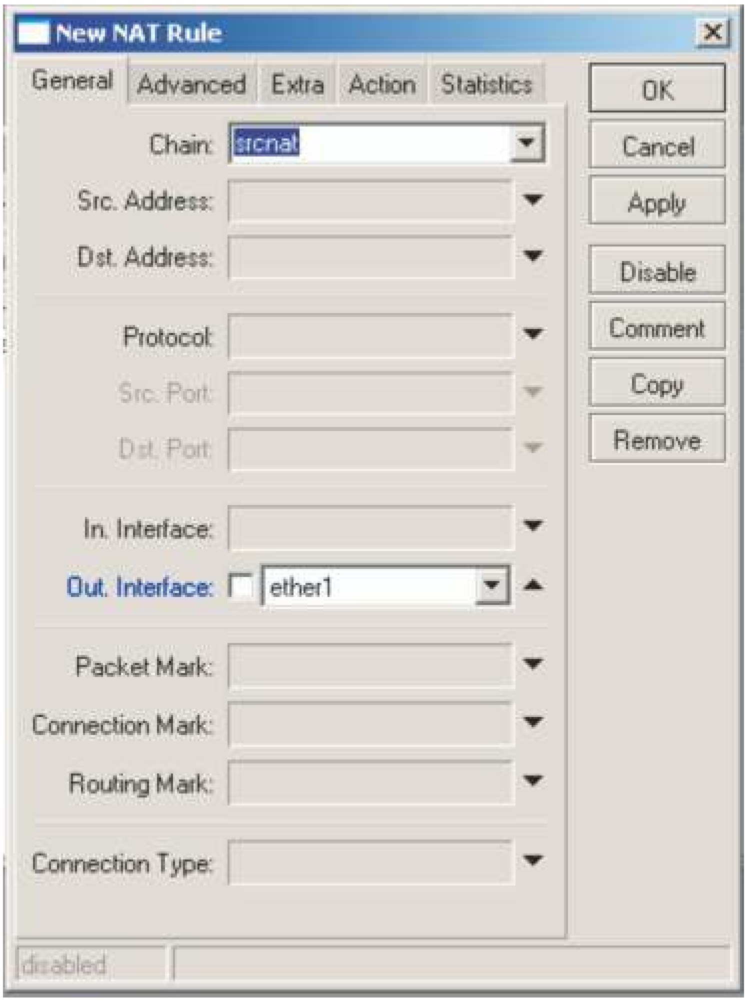


9) Click on IP -> Firewall

10) Click on the NAT tab

11) Click on the red '+' to add a new NAT rule

12) Select Chain -> srcnat, Out Interface -> ether1

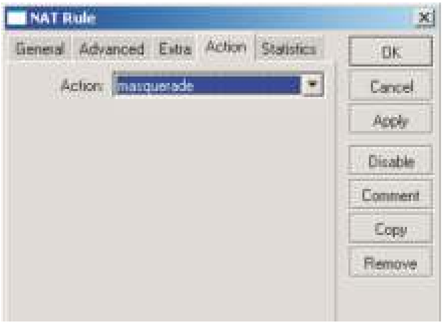


Chain: srcnat

Out. Interface: □ ether1

13) Click on the action tab

14) Select masquerade from the Action list box

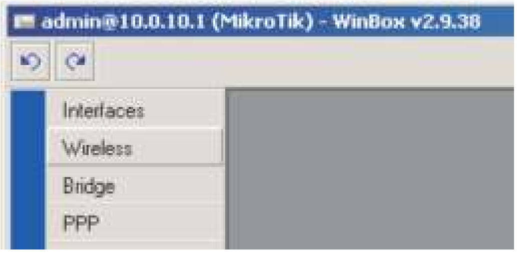


Action: masquerade

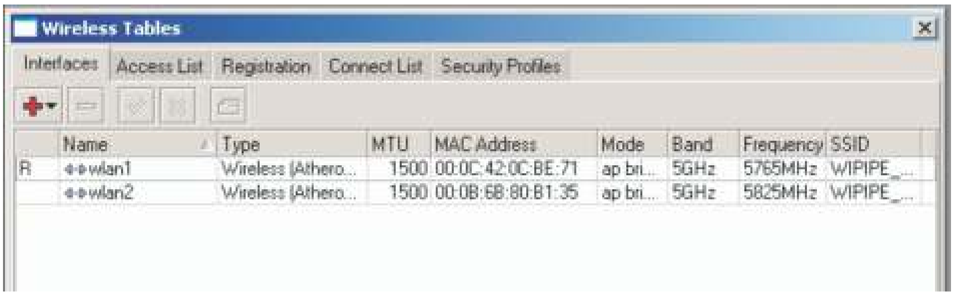
15) Click on ok to save

3. Adding WPA / WPA2 Security to your AP

1) Click on the wireless button

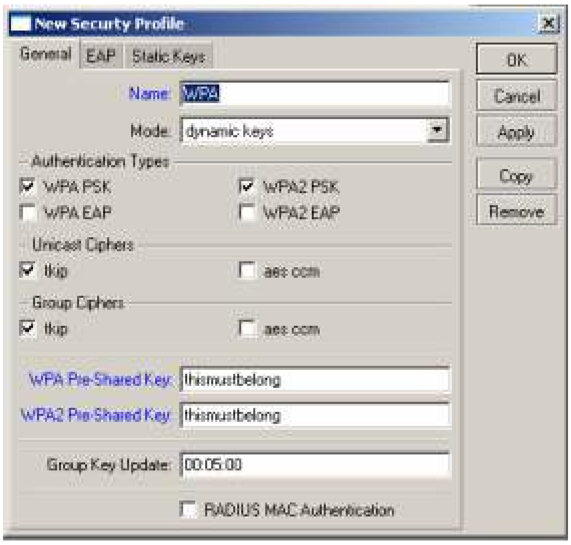


2) Click on the Security Profiles tab



	Name	Type	MTU	MAC Address	Mode	Band	Frequency	SSID
R	wlan1	Wireless (Athero...	1500	00:0C:42:0C:BE:71	ap bri...	5GHz	5765MHz	WIPIPE_...
	wlan2	Wireless (Athero...	1500	00:0B:6B:80:B1:35	ap bri...	5GHz	5825MHz	WIPIPE_...

3) Click on the red '+' to add a new profile
4) Enter a name for the profile in the name field
5) Enter the WPA pass phrase in the WPA pre-shared key field
6) Enter the WPA2 pass phrase in the WPA2 pre-shared key field



Name: WPA

Mode: dynamic keys

Authentication Types

☑ WPA PSK ☑ WPA2 PSK

□ WPA EAP □ WPA2 EAP

Unicast Ciphers

☑ tkip □ aes ccm

Group Ciphers

☑ tkip □ aes ccm

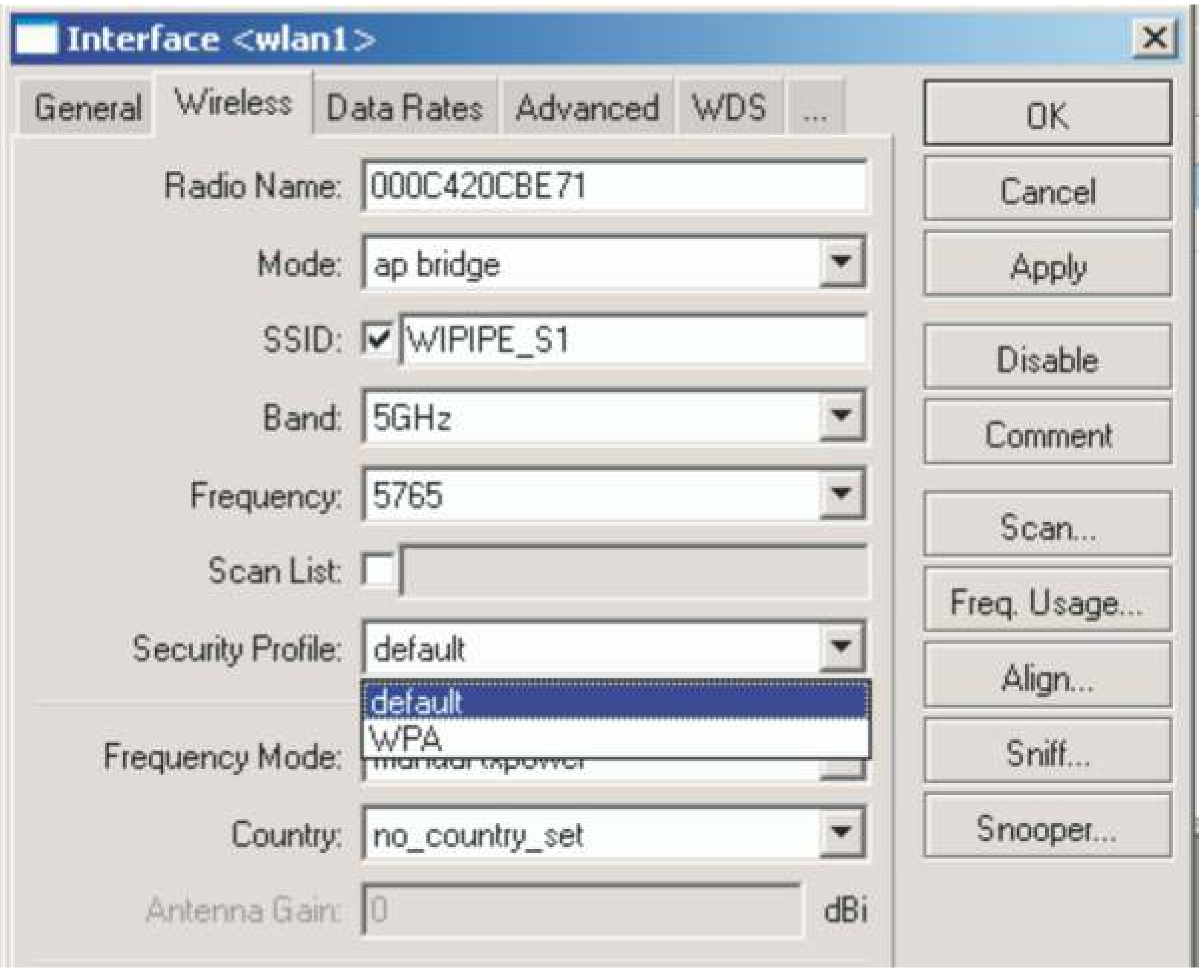
WPA Pre-Shared Key: thismustbelong

WPA2 Pre-Shared Key: thismustbelong

Group Key Update: 00:05:00

□ RADIUS MAC Authentication

7) Click on ok to save
8) Click on the Interfaces tab
9) Double click on wlan1 to configure
10) Click on the wireless tab
11) In the security drop down select the new security profile
12) Click on ok to save



Interface <wlan1>

Radio Name: 000C420CBE71

Mode: ap bridge

SSID: ☑ WIPIPE_S1

Band: 5GHz

Frequency: 5765

Scan List: □

Security Profile: default

Frequency Mode: manual txpower

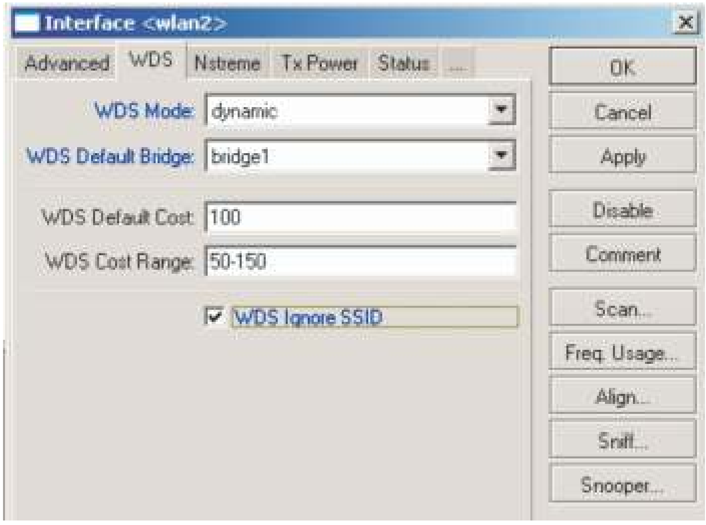
Country: no_country_set

Antenna Gain: 0 dBi

4. Setting up a WDS Bridge

1) Click on Bridge
2) Click on the red '+' to add a new bridge
3) Enter details and click on ok
4) Click on Wireless
5) Double click on the wireless interface to configure
6) Select the wireless tab
7) In the mode drop down select bridge
8) In the band drop down select 5GHz or 2.4GHz-b as appropriate
9) In the Frequency enter the desired frequency
10) Click on the WDS tab
11) In the WDS mode tab select static
12) In the WDS default bridge drop down select the bridge created in step 2 above

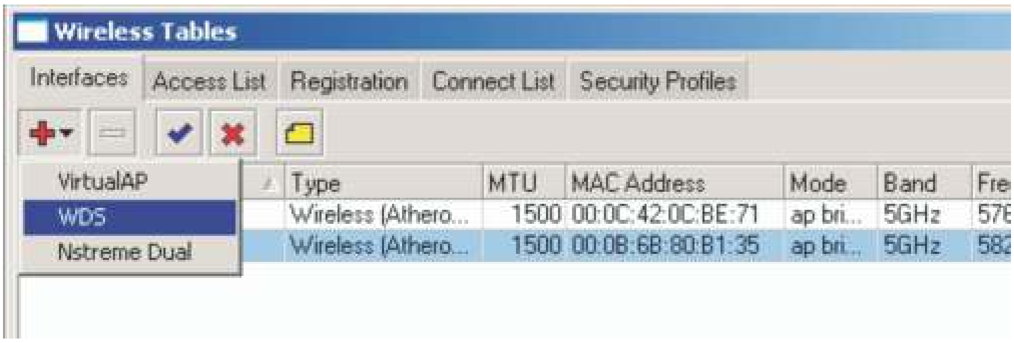
13) Check the WDS Ignore SSID check box



WDS Mode: dynamic
WDS Default Bridge: bridge1
WDS Default Cost: 100
WDS Cost Range: 50-150
☑ WDS Ignore SSID

14) Click on ok to save changes

15) Click on the red '+' and select WDS to add a new WDS interface



Type	MTU	MAC Address	Mode	Band	Fre
Wireless (Athero...	1500	00:0C:42:0C:BE:71	ap bri...	5GHz	576
Wireless (Athero...	1500	00:0B:6B:80:B1:35	ap bri...	5GHz	582

16) Click on the WDS tab

17) From the Master Interface tab select the desired wireless interface

18) Enter the MAC address of the other side of the link in the WDS address field

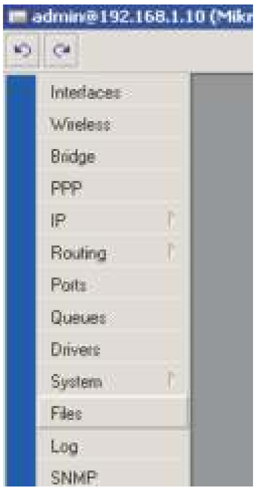
19) Click on ok to save

20) Repeat steps on second AP to create the bridge connection.

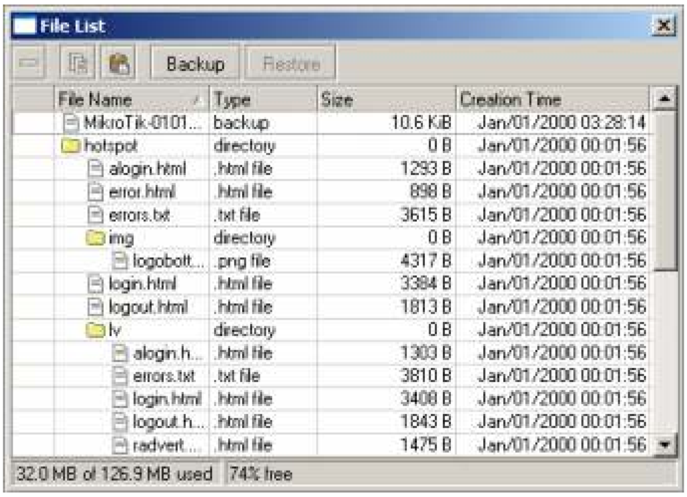
5. Backing up and Restoring AP configurations

To backup your configuration:

1) Click on files



2) Click on backup



File List

Backup | Restore

File Name	Type	Size	Creation Time
MikroTik-0101...	backup	10.6 KiB	Jan/01/2000 03:28:14
hotspot	directory	0 B	Jan/01/2000 00:01:56
alogin.html	.html file	1293 B	Jan/01/2000 00:01:56
error.html	.html file	898 B	Jan/01/2000 00:01:56
errors.txt	.txt file	3615 B	Jan/01/2000 00:01:56
img	directory	0 B	Jan/01/2000 00:01:56
logobott...	.png file	4317 B	Jan/01/2000 00:01:56
login.html	.html file	3384 B	Jan/01/2000 00:01:56
logout.html	.html file	1813 B	Jan/01/2000 00:01:56
lv	directory	0 B	Jan/01/2000 00:01:56
alogin.h...	.html file	1303 B	Jan/01/2000 00:01:56
errors.txt	.txt file	3810 B	Jan/01/2000 00:01:56
login.html	.html file	3408 B	Jan/01/2000 00:01:56
logout.h...	.html file	1843 B	Jan/01/2000 00:01:56
radvert...	.html file	1475 B	Jan/01/2000 00:01:56

32.0 MB of 126.9 MB used | 74% free

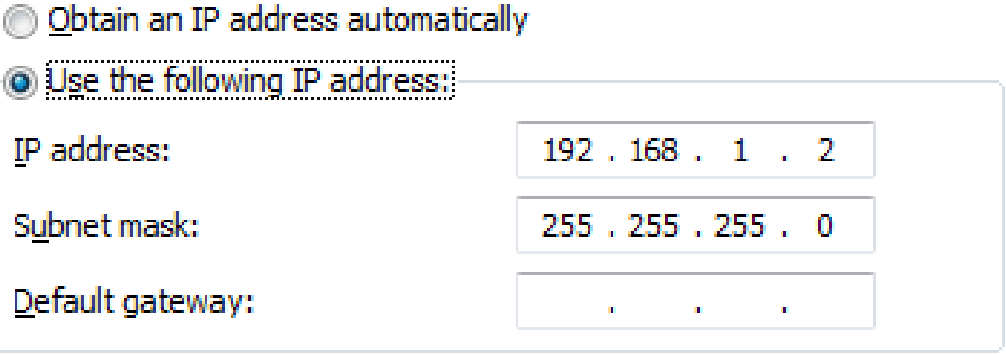
3) The system configuration will automatically be saved
4) To download the file, ftp to the router and download the file

To restore your configuration:

1) Open an ftp connection to the router and upload the configuration file
2) Click on files
3) Select the backup file and click on restore

Example Configuration of EnGenius AP

1. Accessing the EnGenius AP: Engenus's default ip address is 192.168.1.1, default username and password is admin, admin. We should assign the IP address of computer to the same subnet. And access the radio device using any browser.



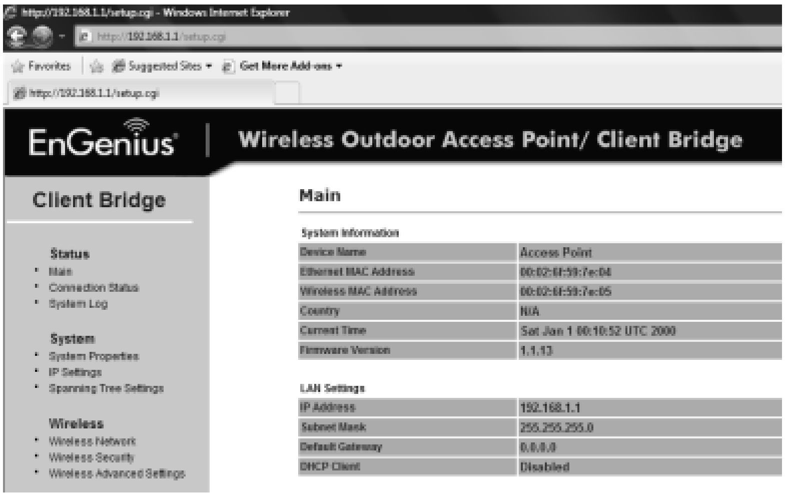
○ Obtain an IP address automatically

● Use the following IP address:

IP address: 192 . 168 . 1 . 2

Subnet mask: 255 . 255 . 255 . 0

Default gateway: . . .



Main

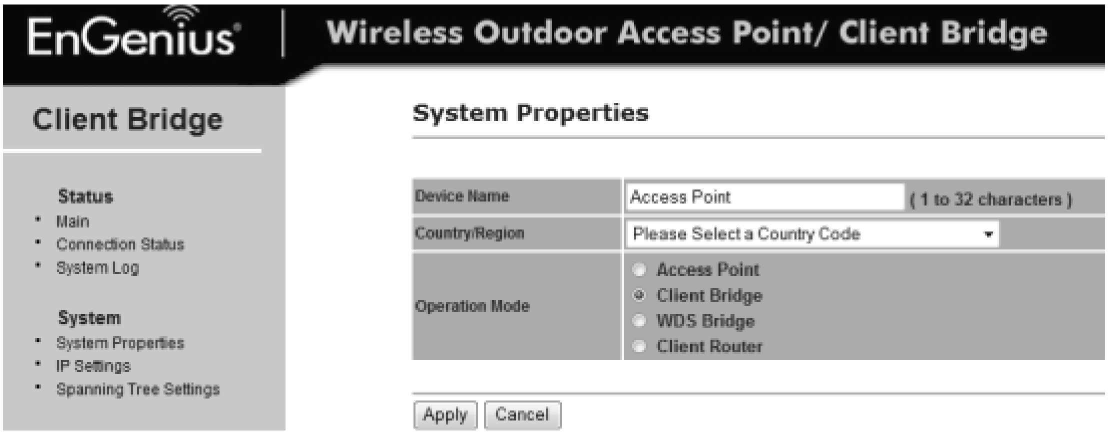
System Information

Device Name	Access Point
Ethernet MAC Address	00:02:6f:59:7e:04
Wireless MAC Address	00:02:6f:59:7e:05
Country	N/A
Current Time	Sat Jan 1 00:10:52 UTC 2000
Firmware Version	1.1.13

LAN Settings

IP Address	192.168.1.1
Subnet Mask	255.255.255.0
Default Gateway	0.0.0.0
DHCP Client	Disabled

Go to System Properties and configure the radio device according to your need like Access Point or Client Bridge, but do not forget to locate your country/region.

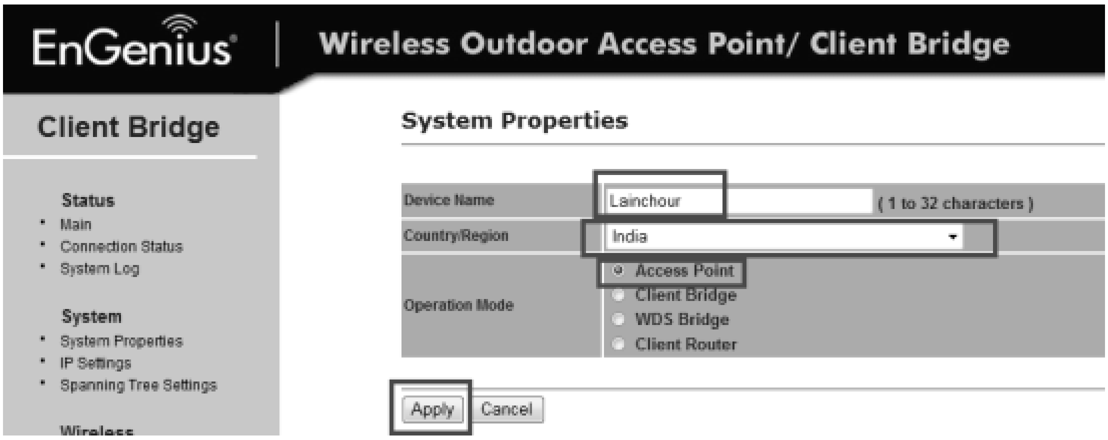


System Properties

Device Name: Access Point (1 to 32 characters)

Country/Region: Please Select a Country Code

Operation Mode: ○ Access Point ● Client Bridge ○ WDS Bridge ○ Client Router



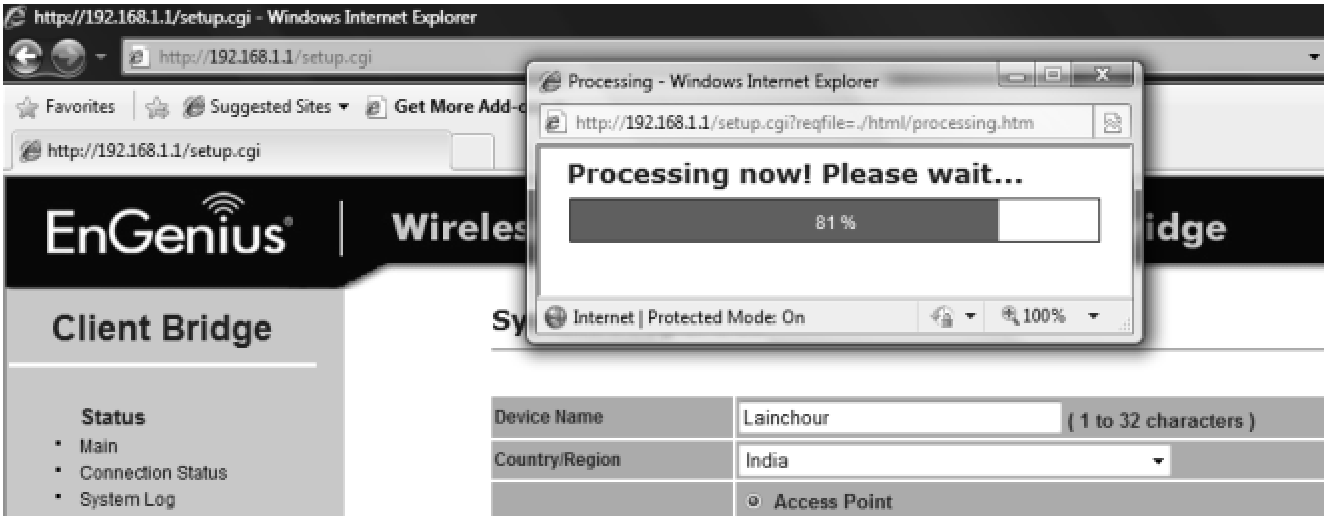
System Properties

Device Name: Lainchour (1 to 32 characters)

Country/Region: India

Operation Mode: ● Access Point ○ Client Bridge ○ WDS Bridge ○ Client Router

Wait until the process complete


http://192.168.1.1/setup.cgi - Windows Internet Explorer
http://192.168.1.1/setup.cgi
Favorites
Suggested Sites
Get More Add-o
http://192.168.1.1/setup.cgi
Processing - Windows Internet Explorer
http://192.168.1.1/setup.cgi?reqfile=./html/processing.htm
Internet | Protected Mode: On
100%
EnGenius
Wireles
idge
Client Bridge
Status
Main
Connection Status
System Log
Sy

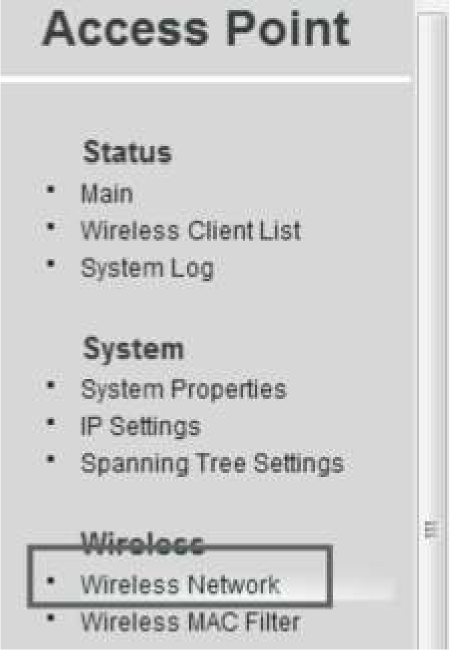
Processing now! Please wait...

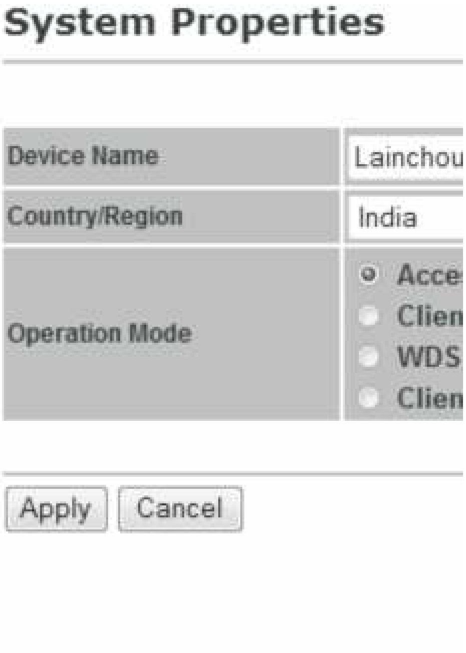
81 %

Device Name: Lainchour (1 to 32 characters)

Country/Region: India

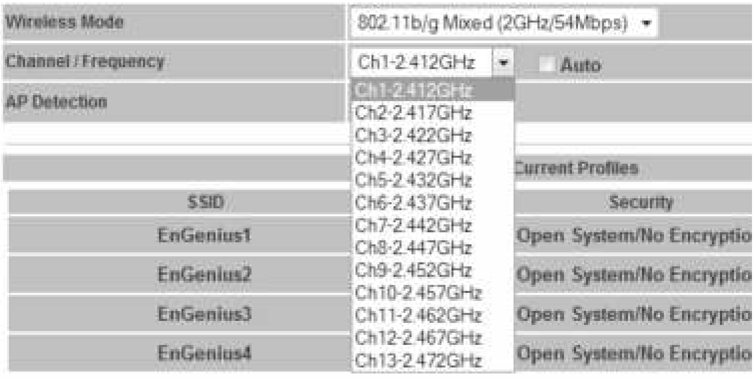
● Access Point




System Properties

Device Name	Lainchou
Country/Region	India
Operation Mode	● Acce ○ Clien ○ WDS ○ Clien

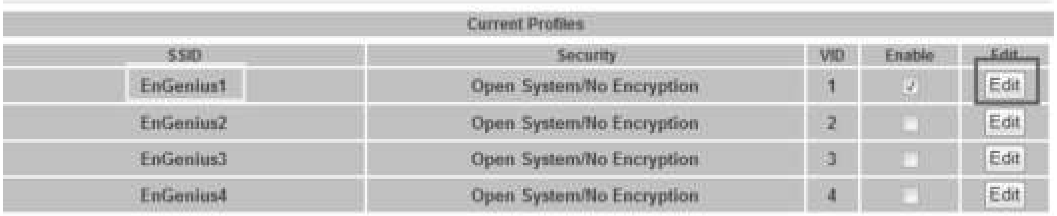
Go to the wireless menu and select the frequency, SSID, and do not forget to give the security profile WPA2/PSK is preferred


Wireless Mode	802.11b/g Mixed (2GHz/54Mbps)
Channel / Frequency	Ch1-2.412GHz □ Auto
AP Detection	

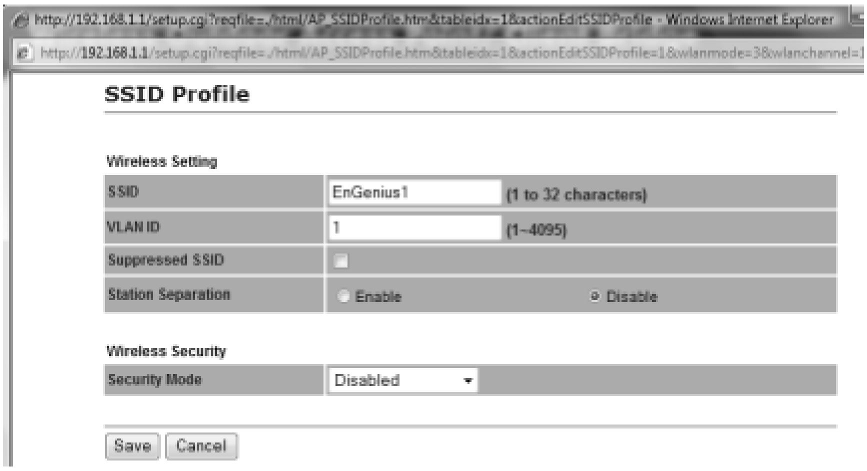
Current Profiles

SSID	Security
EnGenius1	Open System/No Encryptio
EnGenius2	Open System/No Encryptio
EnGenius3	Open System/No Encryptio
EnGenius4	Open System/No Encryptio

To give new SSID and security profile please follow as given below


Current Profiles

SSID	Security	VID	Enable	Edit
EnGenius1	Open System/No Encryption	1	☑	Edit
EnGenius2	Open System/No Encryption	2	□	Edit
EnGenius3	Open System/No Encryption	3	□	Edit
EnGenius4	Open System/No Encryption	4	□	Edit


http://192.168.1.1/setup.cgi?reqfile=./html/AP_SSIDProfile.htm&tableidx=1&actionEditSSIDProfile - Windows Internet Explorer

http://192.168.1.1/setup.cgi?reqfile=./html/AP_SSIDProfile.htm&tableidx=1&actionEditSSIDProfile=1&wlanmode=3&wlanchannel=1

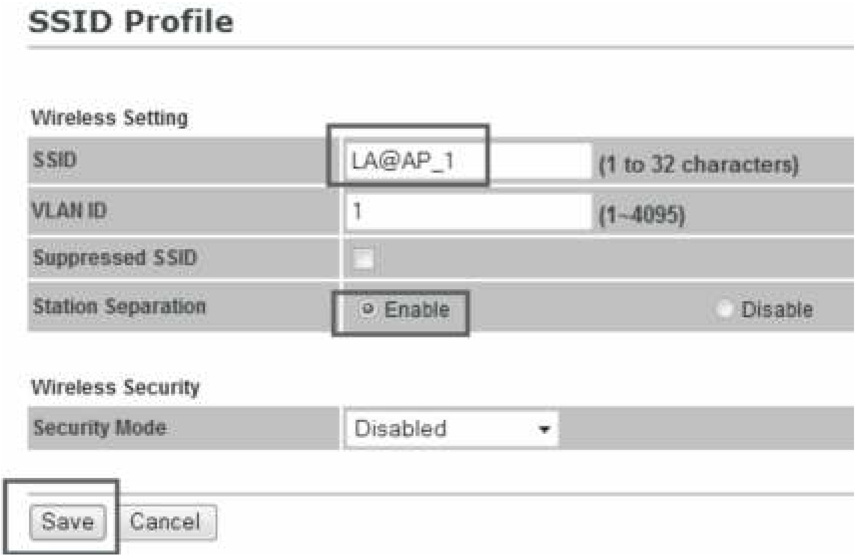
SSID Profile

Wireless Setting

SSID	EnGenius1	(1 to 32 characters)
VLAN ID	1	(1~4095)
Suppressed SSID	□	
Station Separation	○ Enable	● Disable

Wireless Security

Security Mode	Disabled



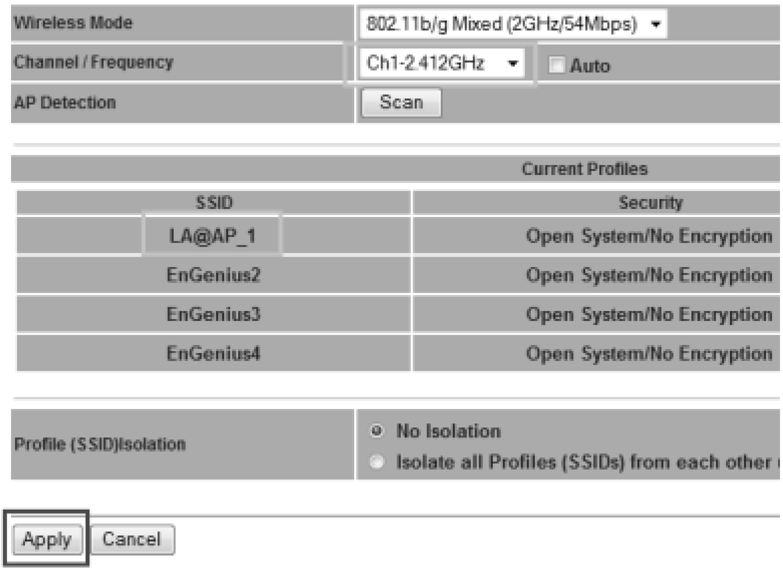
SSID Profile

Wireless Setting

SSID	LA@AP_1	(1 to 32 characters)
VLAN ID	1	(1~4095)
Suppressed SSID	□	
Station Separation	● Enable	○ Disable

Wireless Security

Security Mode	Disabled



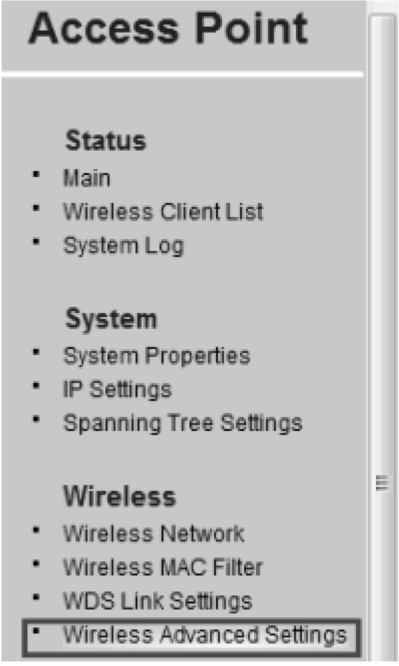
Wireless Mode	802.11b/g Mixed (2GHz/54Mbps)	
Channel / Frequency	Ch1-2.412GHz	□ Auto
AP Detection	Scan	

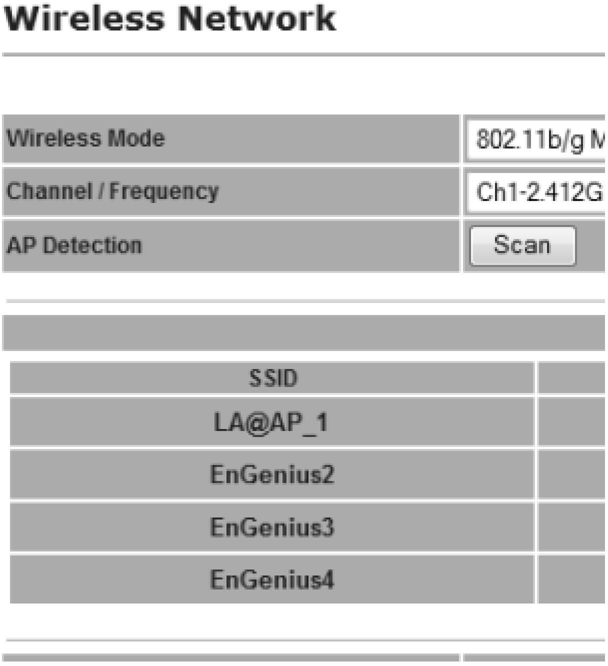
Current Profiles

SSID	Security
LA@AP_1	Open System/No Encryption
EnGenius2	Open System/No Encryption
EnGenius3	Open System/No Encryption
EnGenius4	Open System/No Encryption

Profile (SSID)Isolation: ● No Isolation ○ Isolate all Profiles (SSIDs) from each other

Now go to Wireless Advance Setting



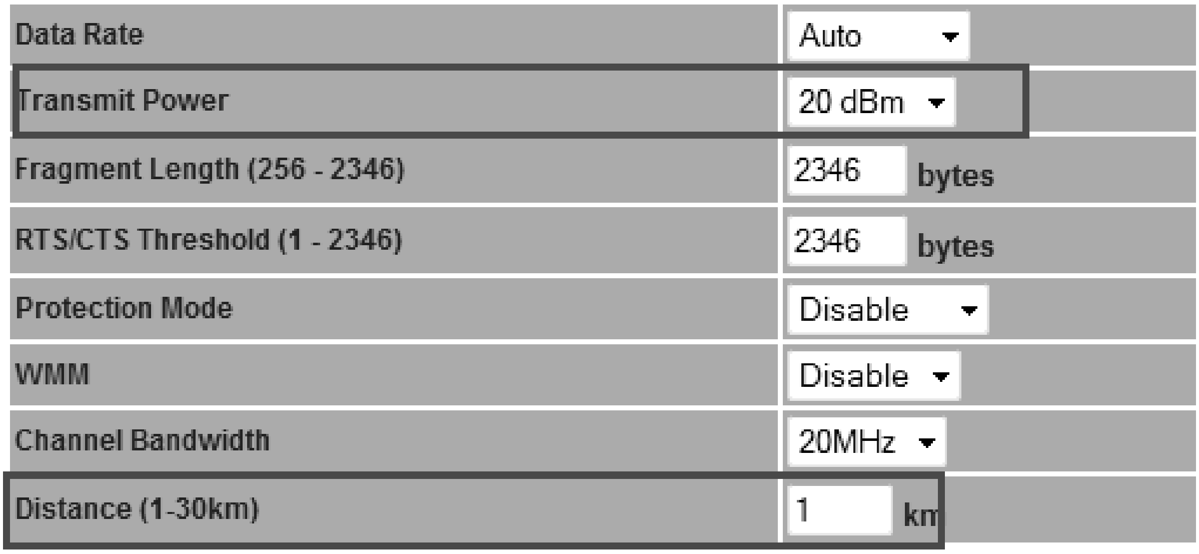


Wireless Network

Wireless Mode	802.11b/g M
Channel / Frequency	Ch1-2.412G
AP Detection	Scan

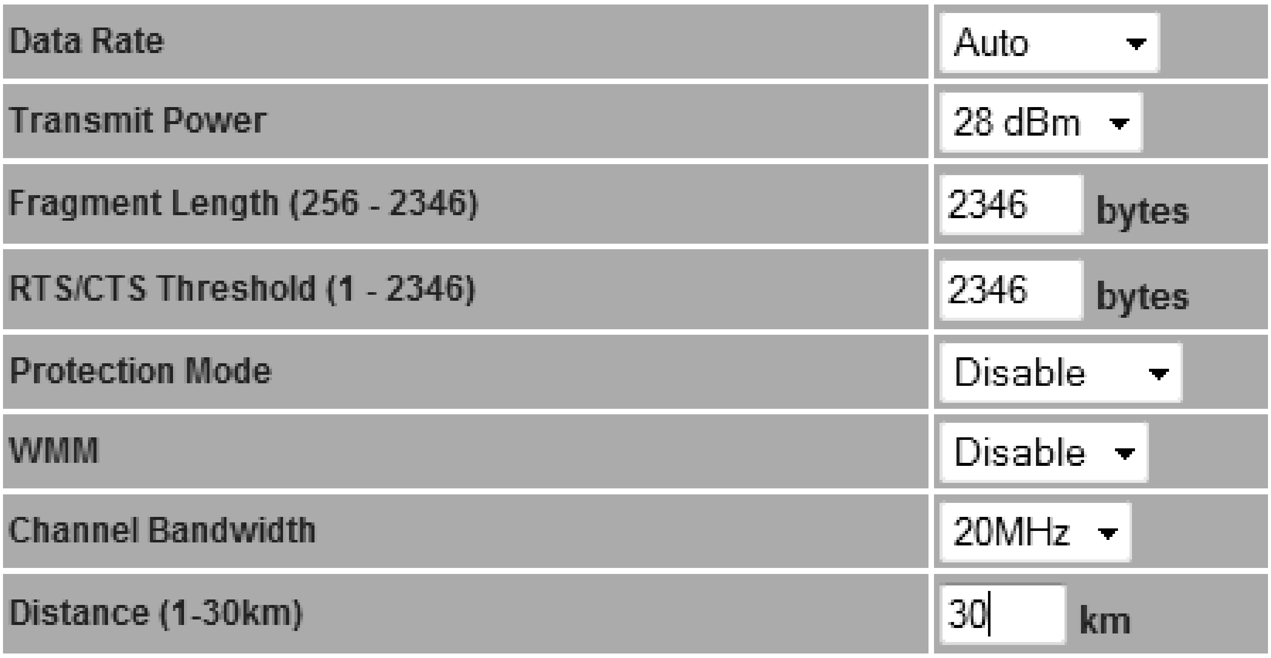
SSID
LA@AP_1
EnGenius2
EnGenius3
EnGenius4

Change the wireless setting like transmit power and expected distance for wireless link.



Data Rate	Auto
Transmit Power	20 dBm
Fragment Length (256 - 2346)	2346 bytes
RTS/CTS Threshold (1 - 2346)	2346 bytes
Protection Mode	Disable
WMM	Disable
Channel Bandwidth	20MHz
Distance (1-30km)	1 km

Engenius device can transmit power up to 30dBm and link up to 30Km



Data Rate	Auto
Transmit Power	28 dBm
Fragment Length (256 - 2346)	2346 bytes
RTS/CTS Threshold (1 - 2346)	2346 bytes
Protection Mode	Disable
WMM	Disable
Channel Bandwidth	20MHz
Distance (1-30km)	30 km

Check list of your Access point configuration

change the operation mode (Access point/Client Bridge)

Select country/region

Name the Access Point where it is located

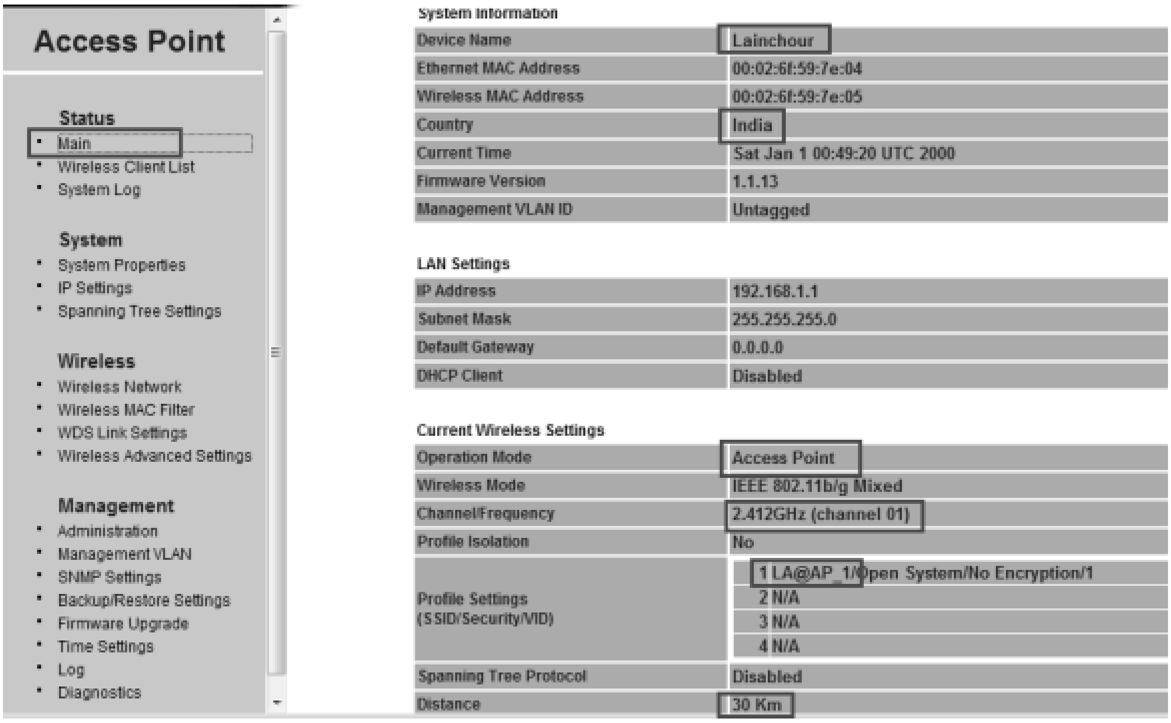
Select the frequency

Name the SSID

Select Transmit Power

Select the distance

Whether something is missing or not, please check the unit according the following figure.



System Information

Device Name	Lainchour
Ethernet MAC Address	00:02:6f:59:7e:04
Wireless MAC Address	00:02:6f:59:7e:05
Country	India
Current Time	Sat Jan 1 00:49:20 UTC 2000
Firmware Version	1.1.13
Management VLAN ID	Untagged

LAN Settings

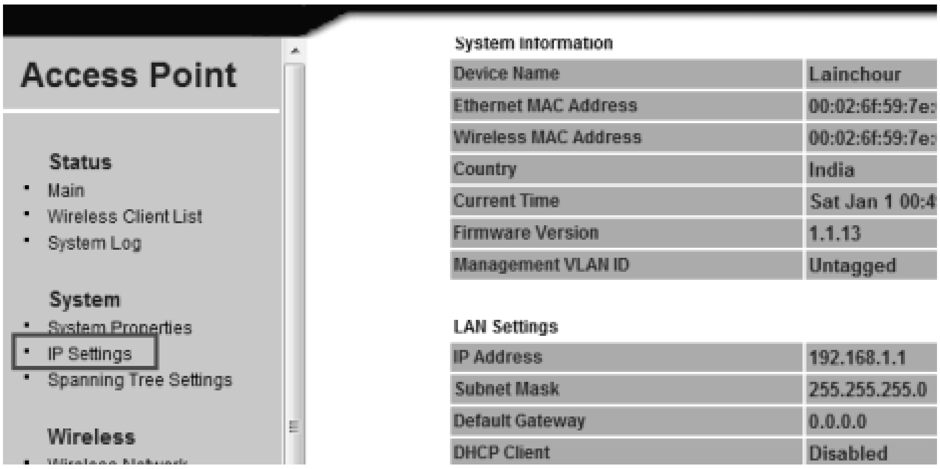
IP Address	192.168.1.1
Subnet Mask	255.255.255.0
Default Gateway	0.0.0.0
DHCP Client	Disabled

Current Wireless Settings

Operation Mode	Access Point
Wireless Mode	IEEE 802.11b/g Mixed
Channel/Frequency	2.412GHz (channel 01)
Profile Isolation	No
Profile Settings (SSID/Security/VID)	1 LA@AP_1/Open System/No Encryption/1 2 N/A 3 N/A 4 N/A
Spanning Tree Protocol	Disabled
Distance	30 Km

IP address Changing of AP Device

Go to ip Setting and configure the ip, subnet, gateway and dns according to given by ISP.

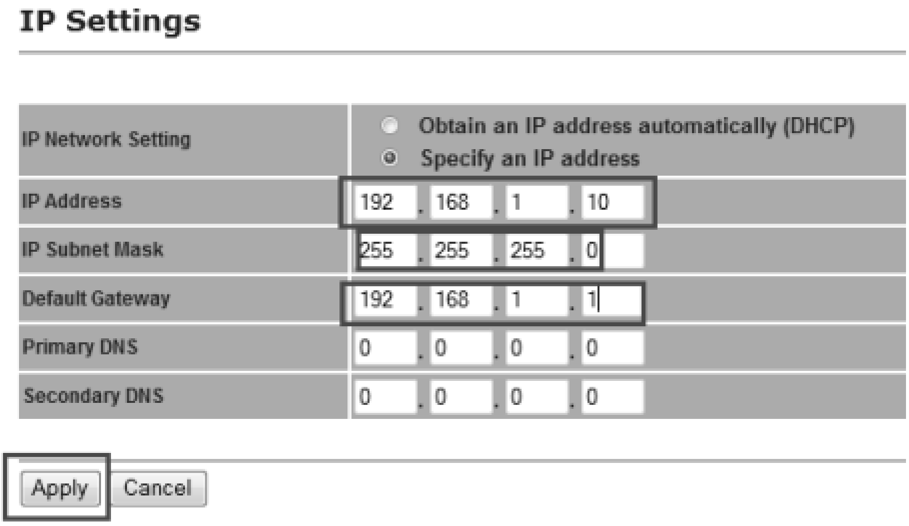


System Information

Device Name	Lainchour
Ethernet MAC Address	00:02:6f:59:7e:
Wireless MAC Address	00:02:6f:59:7e:
Country	India
Current Time	Sat Jan 1 00:4
Firmware Version	1.1.13
Management VLAN ID	Untagged

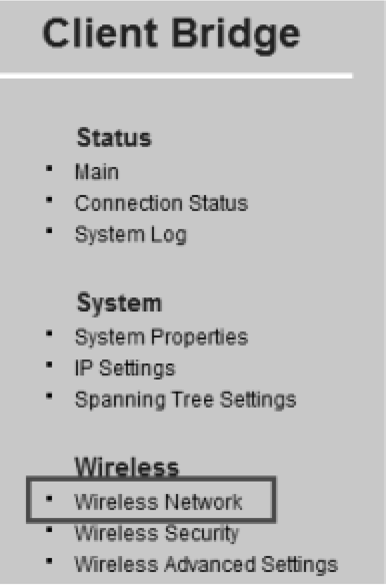
LAN Settings

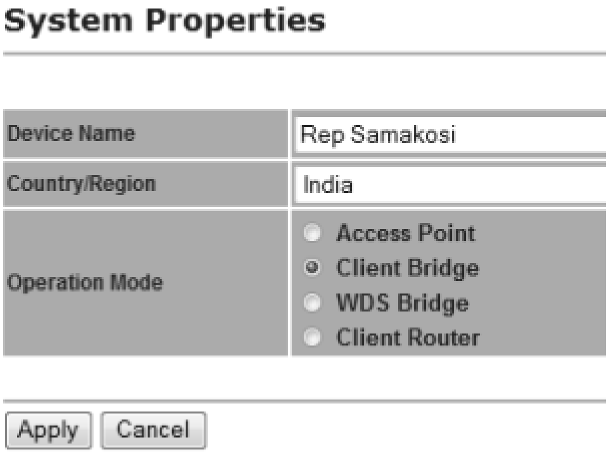
IP Address	192.168.1.1
Subnet Mask	255.255.255.0
Default Gateway	0.0.0.0
DHCP Client	Disabled


IP Settings

IP Network Setting	○ Obtain an IP address automatically (DHCP) ● Specify an IP address
IP Address	192 . 168 . 1 . 10
IP Subnet Mask	255 . 255 . 255 . 0
Default Gateway	192 . 168 . 1 . 1
Primary DNS	0 . 0 . 0 . 0
Secondary DNS	0 . 0 . 0 . 0

2. Connecting To Access Point
   Go to system properties and select the operation mode to client bridge.

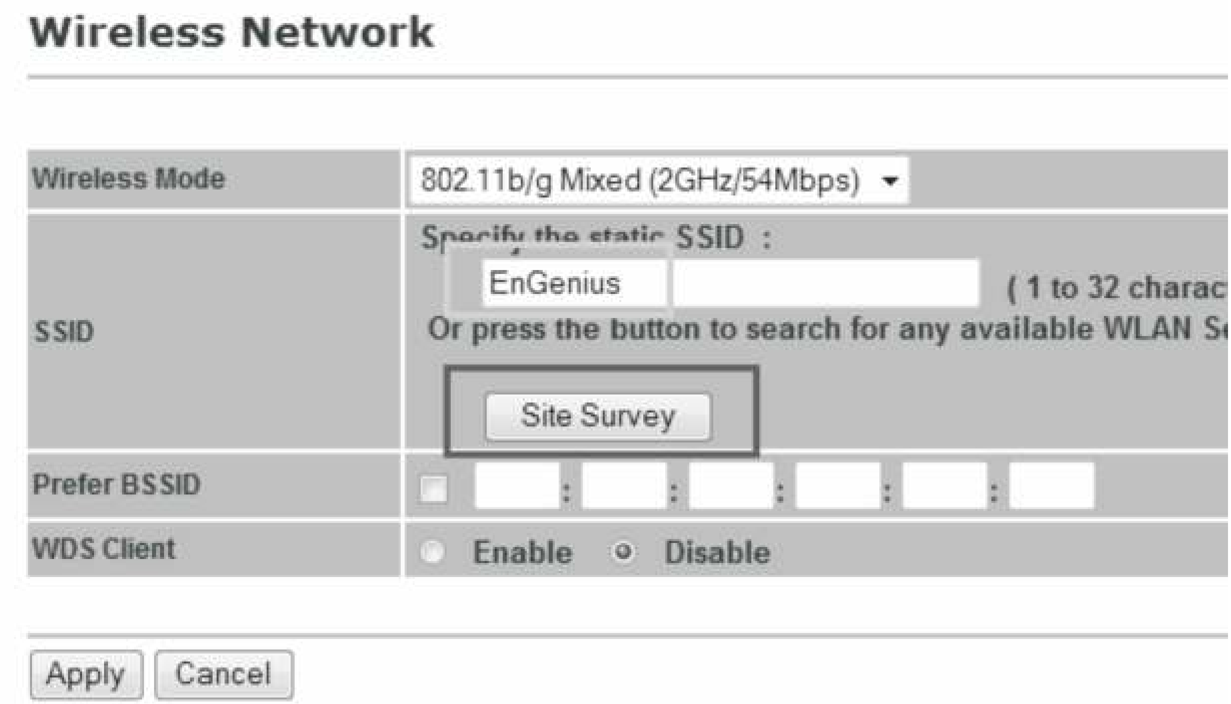




System Properties

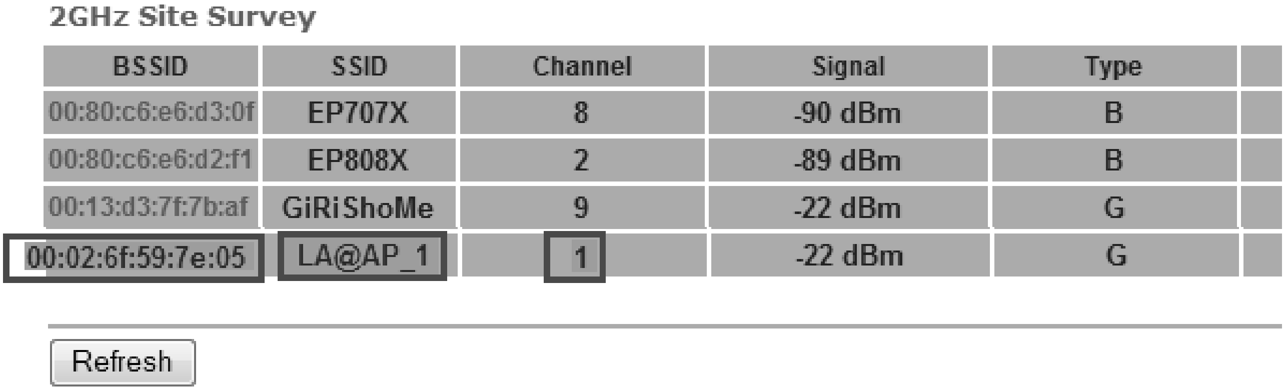
Device Name	Rep Samakosi
Country/Region	India
Operation Mode	○ Access Point ● Client Bridge ○ WDS Bridge ○ Client Router

Then site survey and select the access point by clicking bssid (Mac address of ap)



Wireless Network

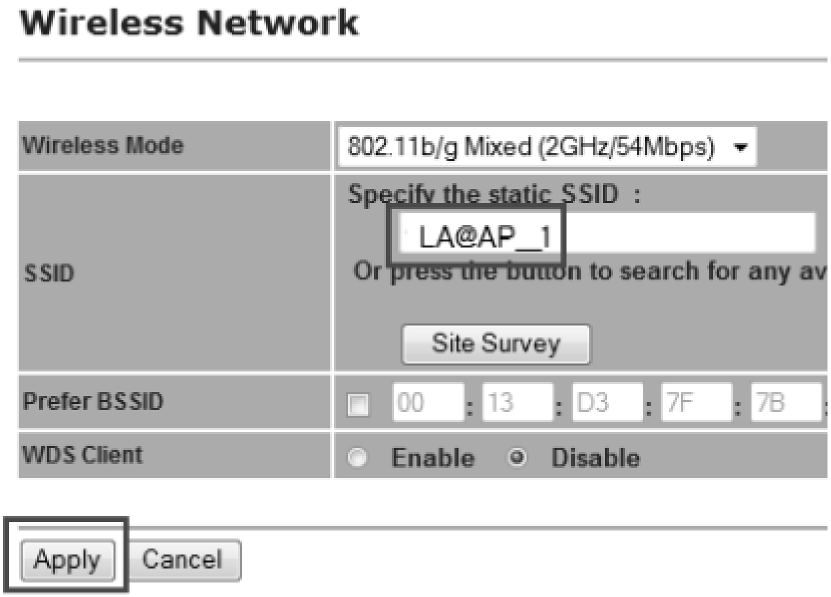
Wireless Mode	802.11b/g Mixed (2GHz/54Mbps)
SSID	Specify the static SSID : EnGenius (1 to 32 charac Or press the button to search for any available WLAN S Site Survey
Prefer BSSID	□ : : : : :
WDS Client	○ Enable ● Disable



2GHz Site Survey

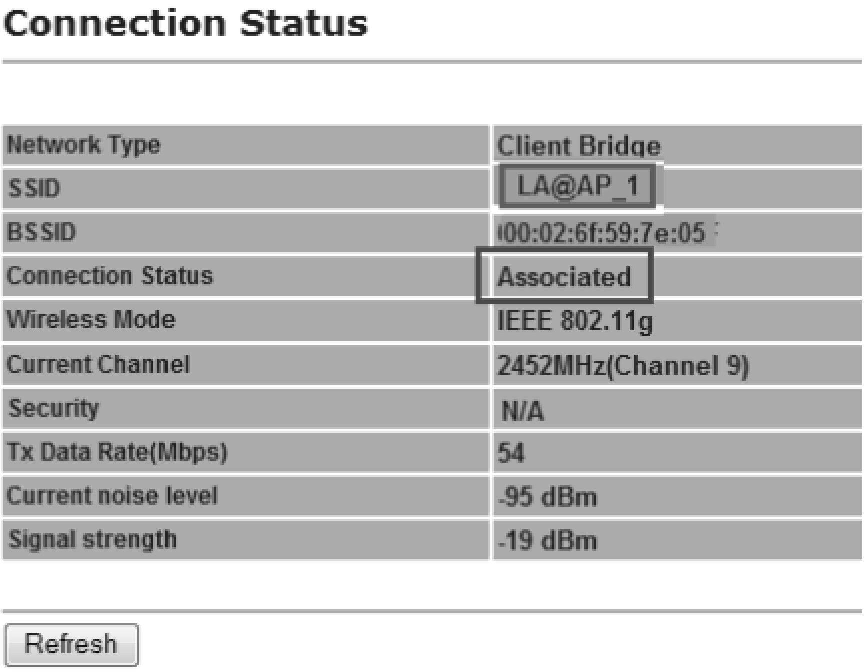
BSSID	SSID	Channel	Signal	Type	
00:80:c6:e6:d3:0f	EP707X	8	-90 dBm	B	
00:80:c6:e6:d2:f1	EP808X	2	-89 dBm	B	
00:13:d3:7f:7b:af	GiRiShoMe	9	-22 dBm	G	
00:02:6f:59:7e:05	LA@AP_1	1	-22 dBm	G	

If the connection status shows as associated then it is confirmed that our client is connected with the access point.



Wireless Network

Wireless Mode	802.11b/g Mixed (2GHz/54Mbps)
SSID	Specify the static SSID : LA@AP_1 Or press the button to search for any av Site Survey
Prefer BSSID	□ 00 : 13 : D3 : 7F : 7B :
WDS Client	○ Enable ● Disable



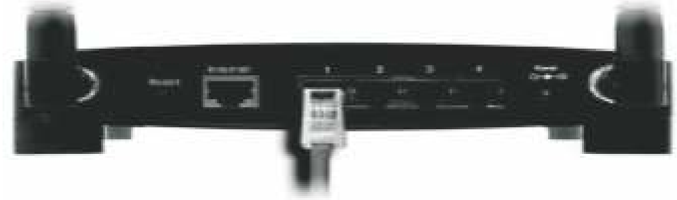
Connection Status

Network Type	Client Bridge
SSID	LA@AP_1
BSSID	00:02:6f:59:7e:05
Connection Status	Associated
Wireless Mode	IEEE 802.11g
Current Channel	2452MHz(Channel 9)
Security	N/A
Tx Data Rate(Mbps)	54
Current noise level	-95 dBm
Signal strength	-19 dBm

Configuration of LinkSys WRT54GL Router

Power the router

Connect the router through LAN port to your computer using straight through cable

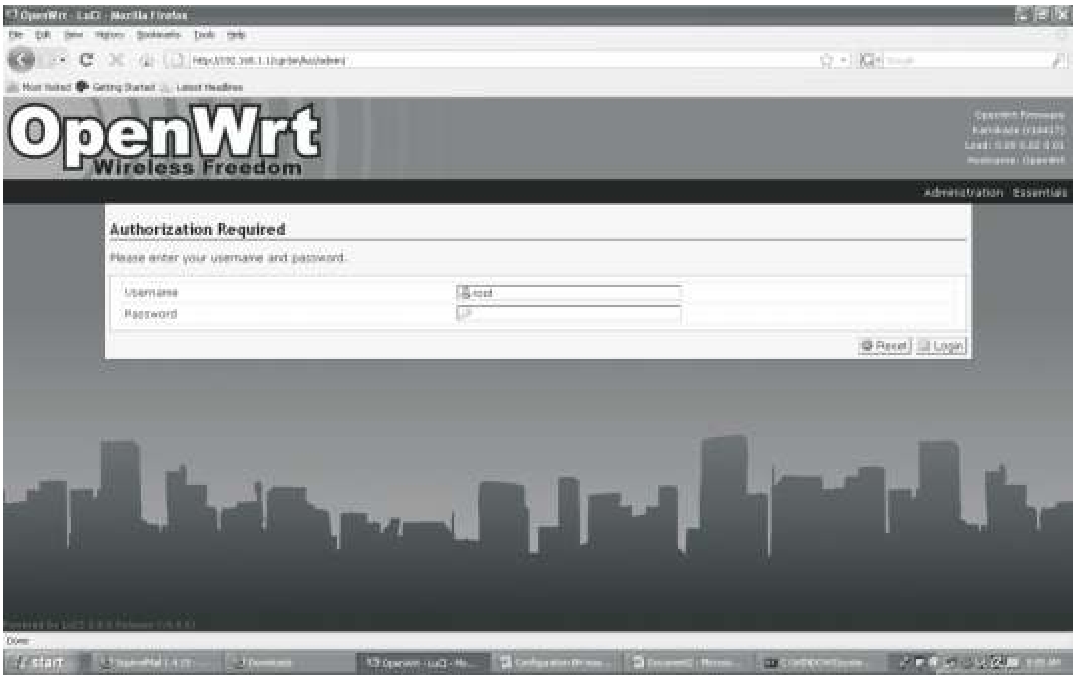


3) The default IP address of router is 192.168.1.1 with the subnet of 255.255.255.0 and default user name is root password admin connect it your computer should be in same subnet

4) Now we can check the connection of router to your computer by ping command for this please follow this Start– Run--- cmd--- ping 192.168.1.1 -t

```
Reply from 192.168.1.1: bytes=32 time=2ms TTL=64
Reply from 192.168.1.1: bytes=32 time=1ms TTL=64
Reply from 192.168.1.1: bytes=32 time=1ms TTL=64
```

5. Now we can browse your router using any browser.



Authorization Required

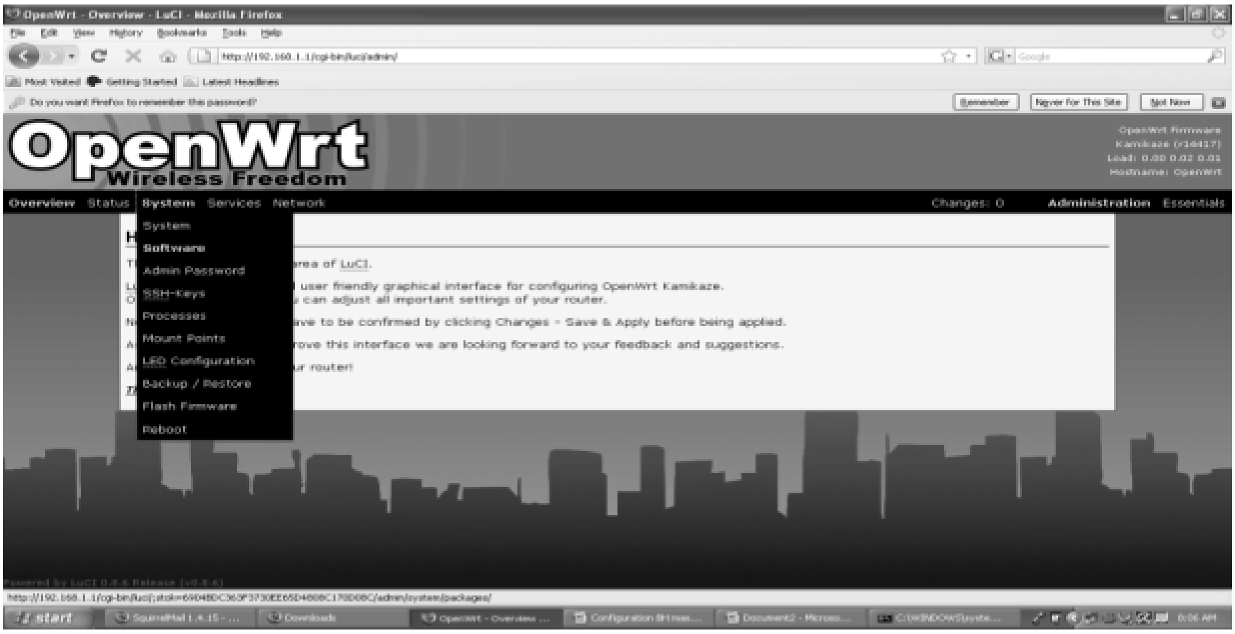
Please enter your username and password.

Username: root

Password:

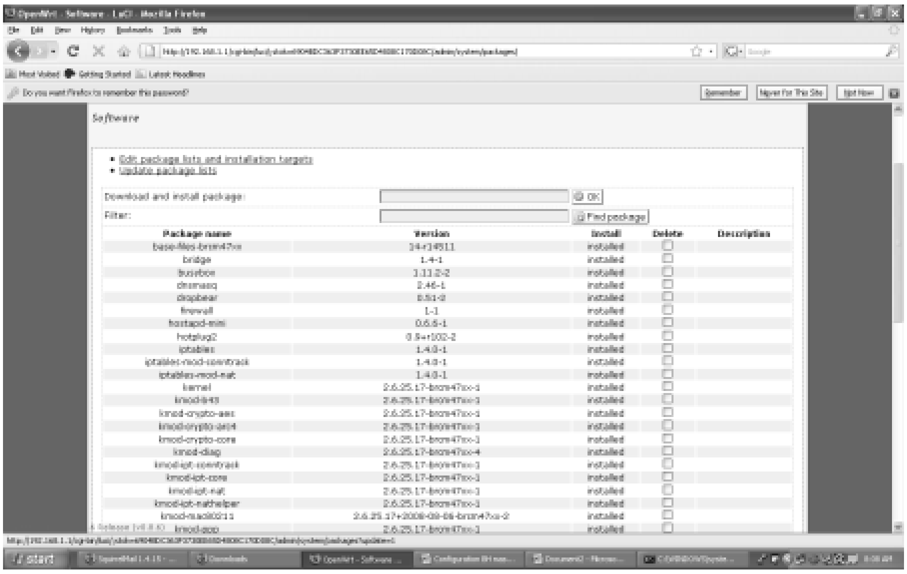
Updating Quagga package M

1. Click on Administration
2. System > Software



http://192.168.1.1/cgi-bin/luci/admin/

3. Click on the package update button and select the quagga –ospfd but be sure that to update this package we must have an internet connection



Software

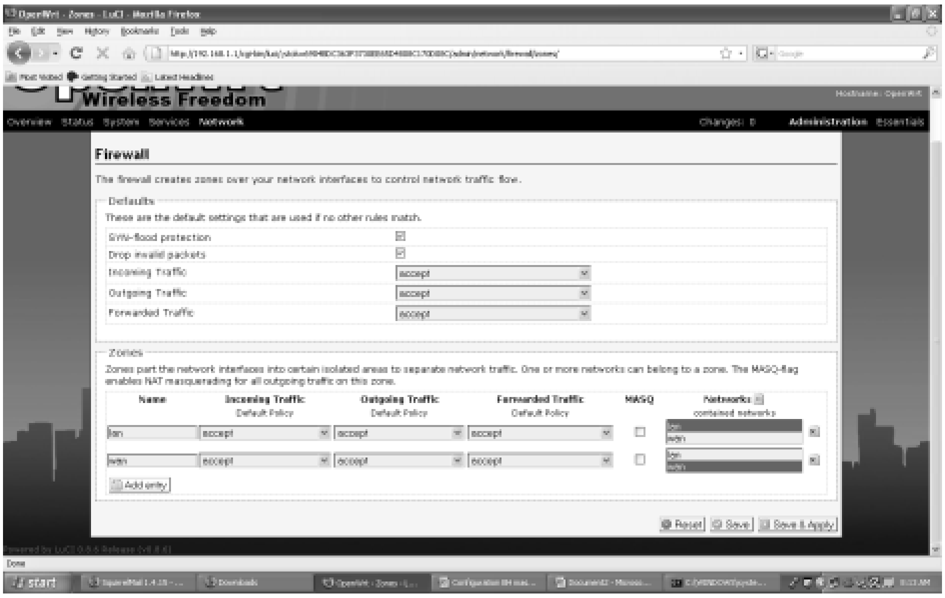
- Edit package lists and installation targets
- Update package lists

Download and install package:

Filter:

Package name	Version	Install	Delete	Description
base-files-brcm47xx	14-r14511	installed	□	
bridge	1.4-1	installed	□	
busybox	1.11.2-2	installed	□	
dnsmasq	2.46-1	installed	□	
dropbear	0.51-2	installed	□	
firewall	1-1	installed	□	
hostapd-mini	0.6.5-1	installed	□	
hotplug2	0.9+r102-2	installed	□	
iptables	1.4.0-1	installed	□	
iptables-mod-conntrack	1.4.0-1	installed	□	
iptables-mod-nat	1.4.0-1	installed	□	
kernel	2.6.25.17-brcm47xx-1	installed	□	
kmod-b43	2.6.25.17-brcm47xx-1	installed	□	
kmod-crypto-aes	2.6.25.17-brcm47xx-1	installed	□	
kmod-crypto-arc4	2.6.25.17-brcm47xx-1	installed	□	
kmod-crypto-core	2.6.25.17-brcm47xx-1	installed	□	
kmod-diag	2.6.25.17-brcm47xx-4	installed	□	
kmod-ipt-conntrack	2.6.25.17-brcm47xx-1	installed	□	
kmod-ipt-core	2.6.25.17-brcm47xx-1	installed	□	
kmod-ipt-nat	2.6.25.17-brcm47xx-1	installed	□	
kmod-ipt-nathelper	2.6.25.17-brcm47xx-1	installed	□	
kmod-mac80211	2.6.25.17+2008-09-08-brcm47xx-2	installed	□	
kmod-ppp	2.6.25.17-brcm47xx-1	installed	□	

4. Disable the NAT as shown below



Firewall

The firewall creates zones over your network interfaces to control network traffic flow.

Defaults

These are the default settings that are used if no other rules match.

SYN-flood protection	☑
Drop invalid packets	☑
Incoming Traffic	accept
Outgoing Traffic	accept
Forwarded Traffic	accept

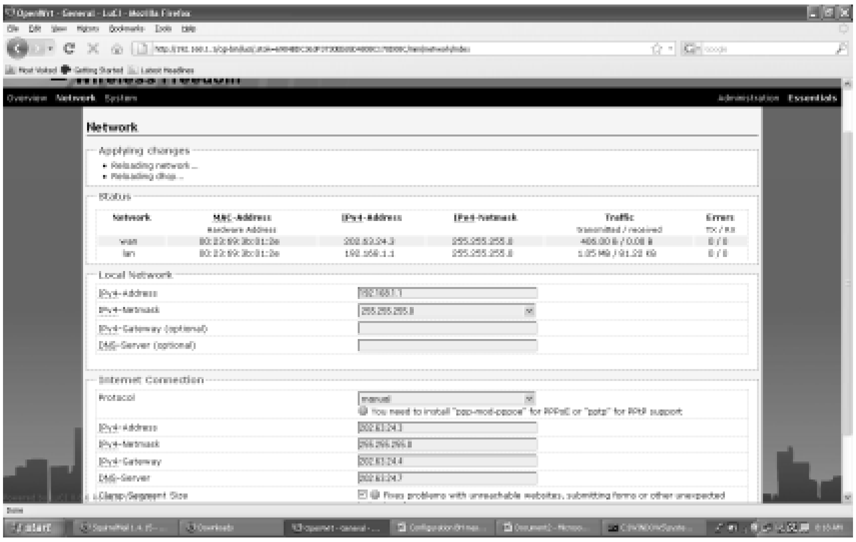
Zones

Zones part the network interfaces into certain isolated areas to separate network traffic. One or more networks can belong to a zone. The MASQ-flag enables NAT masquerading for all outgoing traffic on this zone.

Name	Incoming Traffic Default Policy	Outgoing Traffic Default Policy	Forwarded Traffic Default Policy	MASQ	Networks contained networks
lan	accept	accept	accept	□	lan
wan	accept	accept	accept	□	wan

Wireless Freedom
Overview Status System Services Network
Changes: 0 Administration Essentials
Add entry
Reset Save Save & Apply

5. Essential > network >general and change WAN / LAN IP address provided by your network administrator



Network

Applying changes

- Reloading network ...
- Reloading dhcp ...

Status

Network	MAC-Address Hardware Address	IPv4-Address	IPv4-Netmask	Traffic transmitted / received	Errors TX / RX
wan	00:22:69:3b:01:2e	202.63.24.3	255.255.255.0	406.00 B / 0.00 B	0 / 0
lan	00:22:69:3b:01:2e	192.168.1.1	255.255.255.0	1.05 MB / 91.22 KB	0 / 0

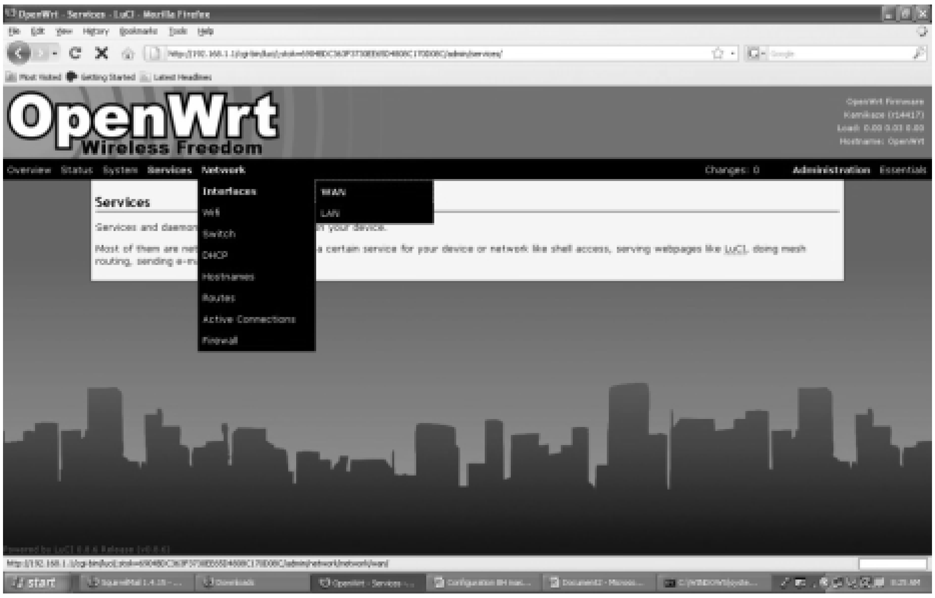
Local Network

IPv4-Address	192.168.1.1
IPv4-Netmask	255.255.255.0
IPv4-Gateway (optional)	
DNS-Server (optional)	

Internet Connection

Protocol	manual You need to install "ppp-mod-pppoe" for PPPoE or "pptp" for PPtP support
IPv4-Address	202.63.24.3
IPv4-Netmask	255.255.255.0
IPv4-Gateway	202.63.24.4
DNS-Server	202.63.24.7
Clamp Segment Size	☑ Fixes problems with unreachable websites, submitting forms or other unexpected

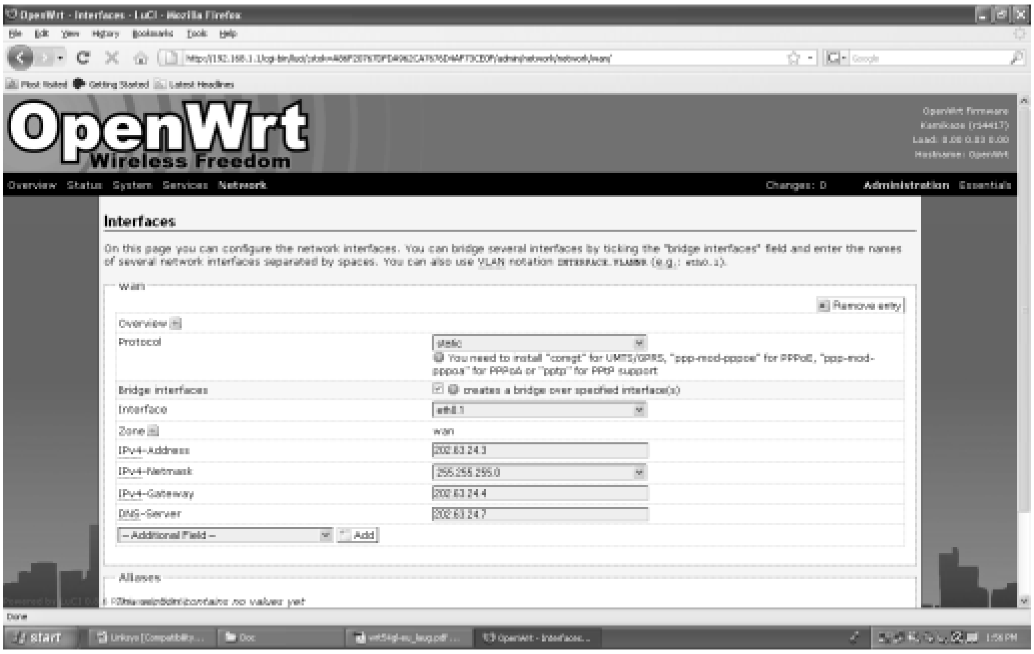
Configuring WAN ip Address


OpenWrt - Services - LuCI - Mozilla Firefox
OpenWrt Wireless Freedom
Overview Status System Services Network
Changes: 0
Administration Essentials
Interfaces
Wifi
Switch
DHCP
Hostnames
Routes
Active Connections
Firewall
WAN
LAN

Services

Services and daemon... on your device.

Most of them are net... a certain service for your device or network like shell access, serving webpages like LuCI, doing mesh routing, sending e-m...


OpenWrt - Interfaces - LuCI - Mozilla Firefox
OpenWrt Wireless Freedom
Overview Status System Services Network
Changes: 0
Administration Essentials
☒ Remove entry
-- Additional Field --
Add

Interfaces

On this page you can configure the network interfaces. You can bridge several interfaces by ticking the "bridge interfaces" field and enter the names of several network interfaces separated by spaces. You can also use VLAN notation INTERFACE.VLANNR (e.g.: eth0.1).

wan

Overview

Protocol: static

You need to install "comgt" for UMTS/GPRS, "ppp-mod-pppoe" for PPPoE, "ppp-mod-pppoa" for PPPoA or "pptp" for PPtP support

Bridge interfaces: ☑ creates a bridge over specified interface(s)

Interface: eth0.1

Zone: wan

IPv4-Address: 202.63.24.3

IPv4-Netmask: 255.255.255.0

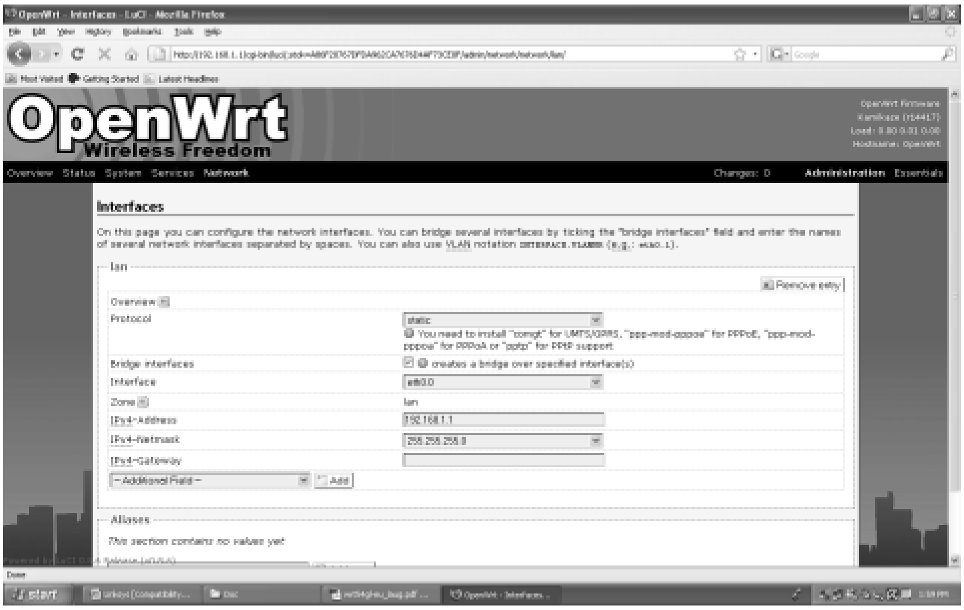
IPv4-Gateway: 202.63.24.4

DNS-Server: 202.63.24.7

Aliases

This section contains no values yet

Configuring LAN IP Address


OpenWrt - Interfaces - LuCI - Mozilla Firefox
OpenWrt Wireless Freedom
Overview Status System Services Network
Changes: 0
Administration Essentials
☒ Remove entry
-- Additional Field --
Add

Interfaces

On this page you can configure the network interfaces. You can bridge several interfaces by ticking the "bridge interfaces" field and enter the names of several network interfaces separated by spaces. You can also use VLAN notation INTERFACE.VLANNR (e.g.: eth0.1).

lan

Overview

Protocol: static

You need to install "comgt" for UMTS/GPRS, "ppp-mod-pppoe" for PPPoE, "ppp-mod-pppoa" for PPPoA or "pptp" for PPtP support

Bridge interfaces: ☑ creates a bridge over specified interface(s)

Interface: eth0.0

Zone: lan

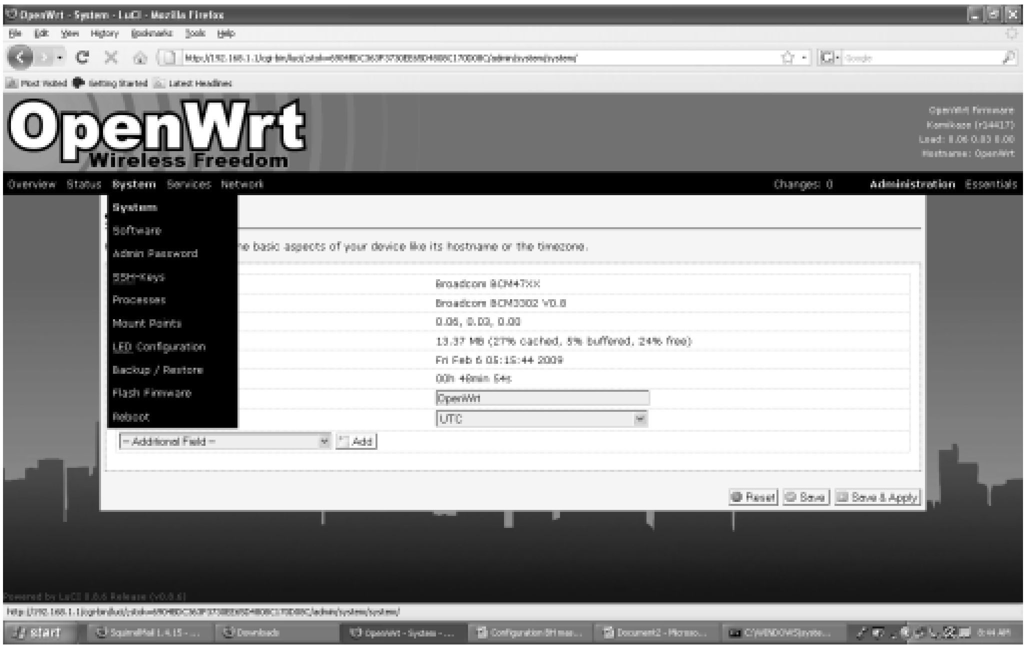
IPv4-Address: 192.168.1.1

IPv4-Netmask: 255.255.255.0

IPv4-Gateway:

Aliases

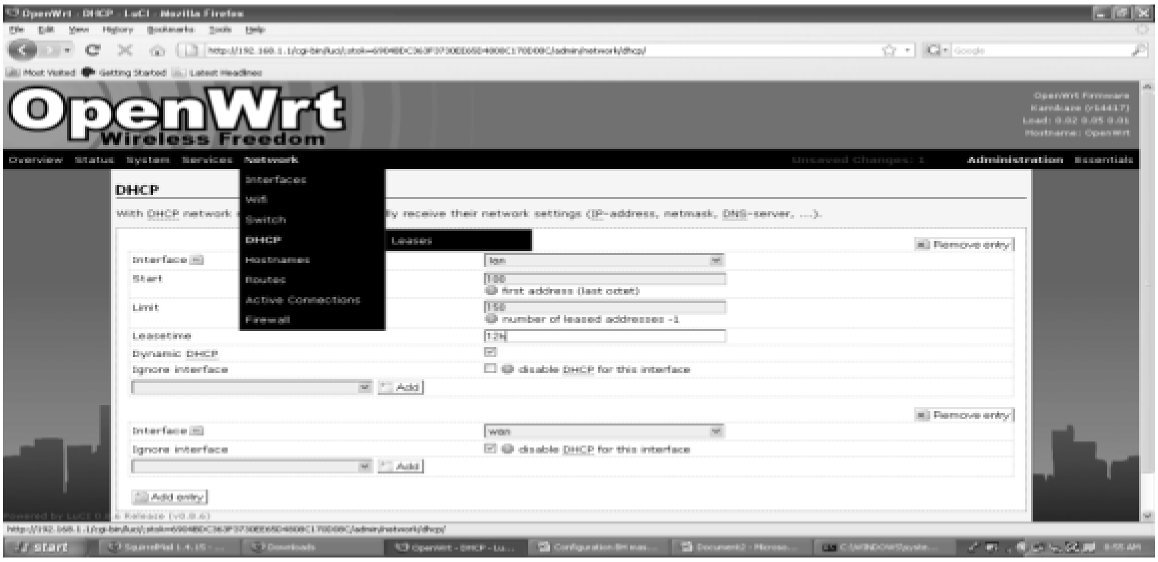
This section contains no values yet



…e basic aspects of your device like its hostname or the timezone.

Broadcom BCM47XX
Broadcom BCM3302 V0.8
0.06, 0.03, 0.00
13.37 MB (27% cached, 5% buffered, 24% free)
Fri Feb 6 05:15:44 2009
00h 46min 54s
OpenWrt
UTC
-- Additional Field -- Add

10. For DHCP configuration Administration>network>dhcp



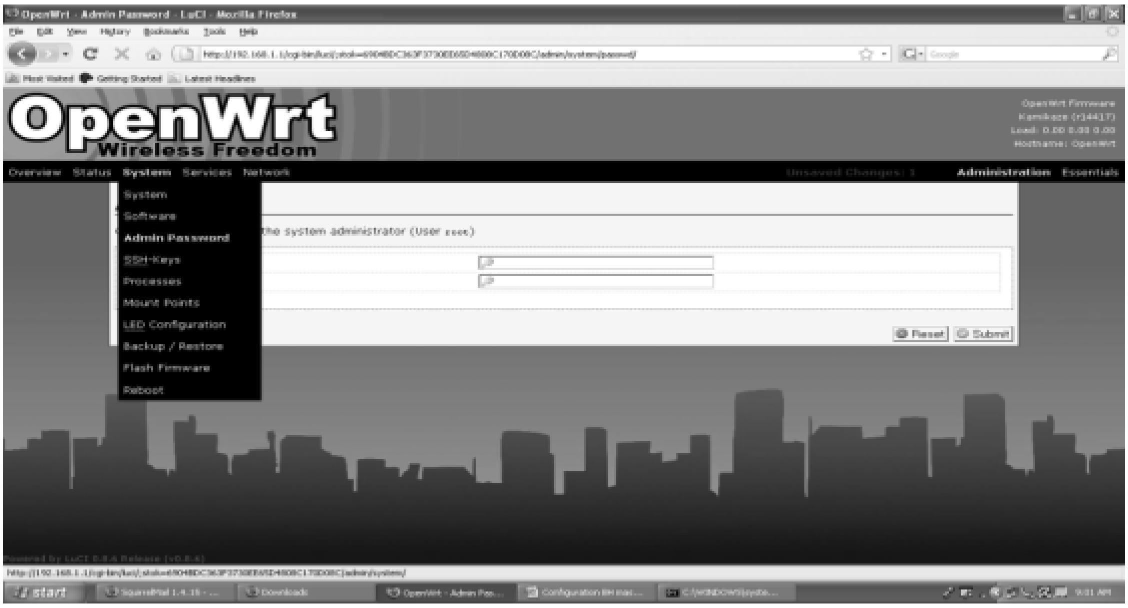
DHCP

With DHCP network … …ly receive their network settings (IP-address, netmask, DNS-server, ...).

Interface: lan
Start: 100 — first address (last octet)
Limit: 150 — number of leased addresses -1
Leasetime: 12h
Dynamic DHCP: ☑
Ignore interface: ☐ disable DHCP for this interface

Interface: wan
Ignore interface: ☑ disable DHCP for this interface

11. To change password: administration>system>admin



…the system administrator (User root)

Troubleshooting of wireless Network

This unit proposes a methodological approach of troubleshooting for wireless networks. The main problem of troubleshooting any communication network is to identify what is going on when things “go wrong”. Rather than rebooting everything that is attached to a power cord or blaming the weather conditions, we propose to follow the OSI model to try to find out the cause of the problem.

The OSI ***(Open Systems Interconnection)*** Reference Model, created by ISO (International Standards Organization), is an abstract description for computer network ***(communication)*** protocol design. The model splits different communication functions into seven different layers that can work independent of each other.

The Internet protocol design follows a similar structure to the OSI model. Each protocol ***layer*** only uses the functionality of the layer below and provides functionality only to layers above.

This structure is of great help when trying to troubleshoot a problem as it helps us to isolate where the problem is. The first thing that we always need to do when things go wrong is to try to identify in which “layer” the problem appears and which layer that is the cause of the problem.

For example, users will always complain that an application “x” is not working (OSI Layer 7) but the cause of the problem can be in any of layers below. It can be related to lack of radio signal (OSI Layer 1) or lack of IP address (OSI Layer 3).

Layer	**OSI**	**TCP/IP**
7	Application	Application
6	Presentation	
5	Session	Transport (TCP)
4	Transport	
3	Network	Network (IP)
2	Data Link	Media Access Control
1	Physical	

OSI model versus TCP/IP protocol suite.

Methodology

Depending on the information that we have in advance we can take two approaches:

Top-down troubleshooting

When there is a “problem”, top-down troubleshooting starts by checking the application's configuration settings and finishes by checking whether there is wireless interference or a low signal level in the radio receiver.

Middle-top, middle-down troubleshooting

When there is a “problem”, this approach starts by checking whether there is IP connectivity to the requested service or the border router, and depending on the result attempts to troubleshoot the layers below or above.

This approach is the most popular, ping <the service>, ping <the router>.

Unfortunately most of the time this only helps to identify who to blame, rather than troubleshooting the actual problem. If “ping” to the border router fails then we can blame the wireless carrier, if “ping” to the service fails then we can blame the international carrier. If none of them fail then we blame the user or the operative system.

Whatever approach we take to troubleshoot a problem, it is important that we should be familiar with the tools that are appropriate when analyzing each of the functional layers of our network.

The ultimate goal of having a methodology is that it will allow we to describe ***troubleshooting procedures*** and be able to identify which problems that require higher levels of expertise.

Practical example

Let's take an example to illustrate the approach. If someone calls we and screams “I can not read my Hotmail!”. We need to be able to have a method to identify the cause without calling in your best network engineer.

If we follow the first of the proposed methods (top-down) we will ask the following questions trying to identify where the problem is:

What program do we use to check your e-mail? (Checking for application problems)

Can we check the proxy settings of your program?

Can we reach any other Internet sites? (Checking for DNS problems)

Does your application time out? (Checking for session TCP problems)

Have we authenticated with the access-control server? (Checking for Authentication Problems)

Can we reach our router/provider web site? (Checking for routability problems)

Do we have an IP address? (Checking for IP problems)

If we follow the second proposed method (middle-top/down) we will ask the following questions:

Can we ping hotmail.com?

Can we ping <IP address of the border router of the WISP>?

If both answers are “no”:

Do we have an IP address?

Have we authenticated with the access-control server?

Classifying problems is not an easy task, and problems vary from network to network but the ***methodology*** we use to troubleshoot is always the same.

There is one easy way to classify any problem in a network:

Things do not work at all (Why my computer does not <include word here>?)
Things work sometimes... (or things work, but “badly”) (Why is my computer so slow?)
The first type of problem is normally easier to troubleshoot, as it stems from problems related to a wrong link budget, power loss in the equipment, misalignment of antennas, wrong settings etc

The second type of problem, especially when related to lower layers of the TCP/IP stack, is more difficult to troubleshoot as it will require we to monitor all the wireless parameters during a period of time while we are trying to identify the cause of the problem.

In the diagram below we include a set of tools that can help we to troubleshoot:

Layer	OSI	TCP/IP	Tools
7	Application	Application	Nslookup Transport (TCP)
6	Presentation		
5	Session	Transport (TCP)	Ntop (Win32/Linux) Visualroute, traceroute
4	Transport		
3	Network	Network (IP)	Nmap Ntop (Win32/Linux) Ethereal Etherape
2	Data Link	Media Access Control	Ethereal (Win32/Linux), Netstumbler (Win32), Kismet, Vendor Specific Management Tools
1	Physical		

Tools for troubleshooting for each and one of the seven layers of the TCP/IP protocol stack.

When it comes to identify problems in the wireless media, we can use two types of tools: the ones that work with any IEEE 802.11b compliant product, and those that come with every specific vendor.

Tools for troubleshooting

- Nslookup, dig
- Ntop
- Visualroute, traceroute
- Nmap
- Ethereal (See Scenario 3)
- Etherape (See Scenario 2)
- Netstumbler (See Scenario 1)
- Kismet
- Vendor specific management tools

Scenario 1: Radio Interferences, Occupied Channels?

There are no simple and cheap way to monitor all the parameters involved in the "physical layer" of your wireless network. When troubleshooting the "radio" we will always use tools that talk with the "wireless cards" and retrieve a limited set of that information for we.

By using a program like "Netstumbler", a wireless cards acts as a simple "spectrum" analyzer that can scan for existing networks, their signal to noise ratio, modulation technique and operation mode. Netstumbler gathers all that information in an easy to use interface.

WEP encryption is enable in the network with SSID=buss. All networks are listened with good SNR ratios SNR>10 dB.Netstumbler is a "passive" software that eavesdrops wireless traffic from the network. Not all the wireless card will allow we to "monitor" wireless traffic promiscuously; before we install Netstumbler check out that your wireless card is supported.

Scenario 2: Congested Network? Flooding?

If we want to get a "general overview" of the type of IP connections that are active in your wireless network, we can use the Unix program "EtherApe" in your wired gateway. EtherApe allows we to monitor the incoming and outgoing connections routed into your wireless. It can help we not only to identify the type of IP traffic present and the distribution of traffic between your nodes but also to identify how “dynamic” your network is. By observing the traffic graphs with the software, we will be able to detect viruses scanning your clients or the present of heavy peer-to-peer or FTP traffic. There are similar software and more sophisticated protocol analyzers also under MS Windows (AirDefense, Scrutinizer, SolarWinds, etc) but few of them are free (if any!).

Scenario 3: Why this network service is not working? Connection Refused?

If we need to have a closer look to what is happening for a specific type of traffic we might consider installing Ethereal. Ethereal will allow we to capture ALL the traffic that is passing by your interface and be able to examine the traffic flows and the bits and bytes of every transaction. Ethereal is very useful to monitor:

Packet loss in TCP connections: That is normally an indication of a congested network, collisions etc. round trip-times: that is an indication of your network latency. High round trip-times inside of your wireless network is an indication of high level of channel utilization or packet collisions.

Protocol Errors: Errors that are not normally visible to the user as inappropriate authentication, duplicate IP addresses, network unreachable, ICMP flooding etc.

References

- Wireless Networking in the Developing World by Rob Flickenger, Corinna “Elektra” Aichele, Sebastian Büttrich, Laura M. Drewett, Alberto Escudero-Pascual, Matt Westervelt, Marco Zennaro, Frédéric Renet, Ermanno Pietrosemoli, Juergen Neumann, , Adam Messer., Gina Kupfermann, Tomas Krag, Kyle Johnston, Ian Howard., Jim Forster, Carlo Fonda

- www.wndw.org

- www.wiki.mikrotik.com

- www.wikipedia.org

- http://tools.ietf.org/html/

- http://www.itrainonline.org/itrainonline/mmtk/

- http://www.antenna-theory.com/antennas/main.php

Notes

Notes

10 YEARS DEF DIGITAL EMPOWERMENT foundation

Digital Empowerment Foundation
House No. 44, 3rd Floor (Next to Naraina IIT Academy)
Kalu Sarai, (Near IIT Flyover), New Delhi - 110016
T: +91 11 26532786   F: +91 11 26532787
E: def@defindia.net   W: www.defindia.net