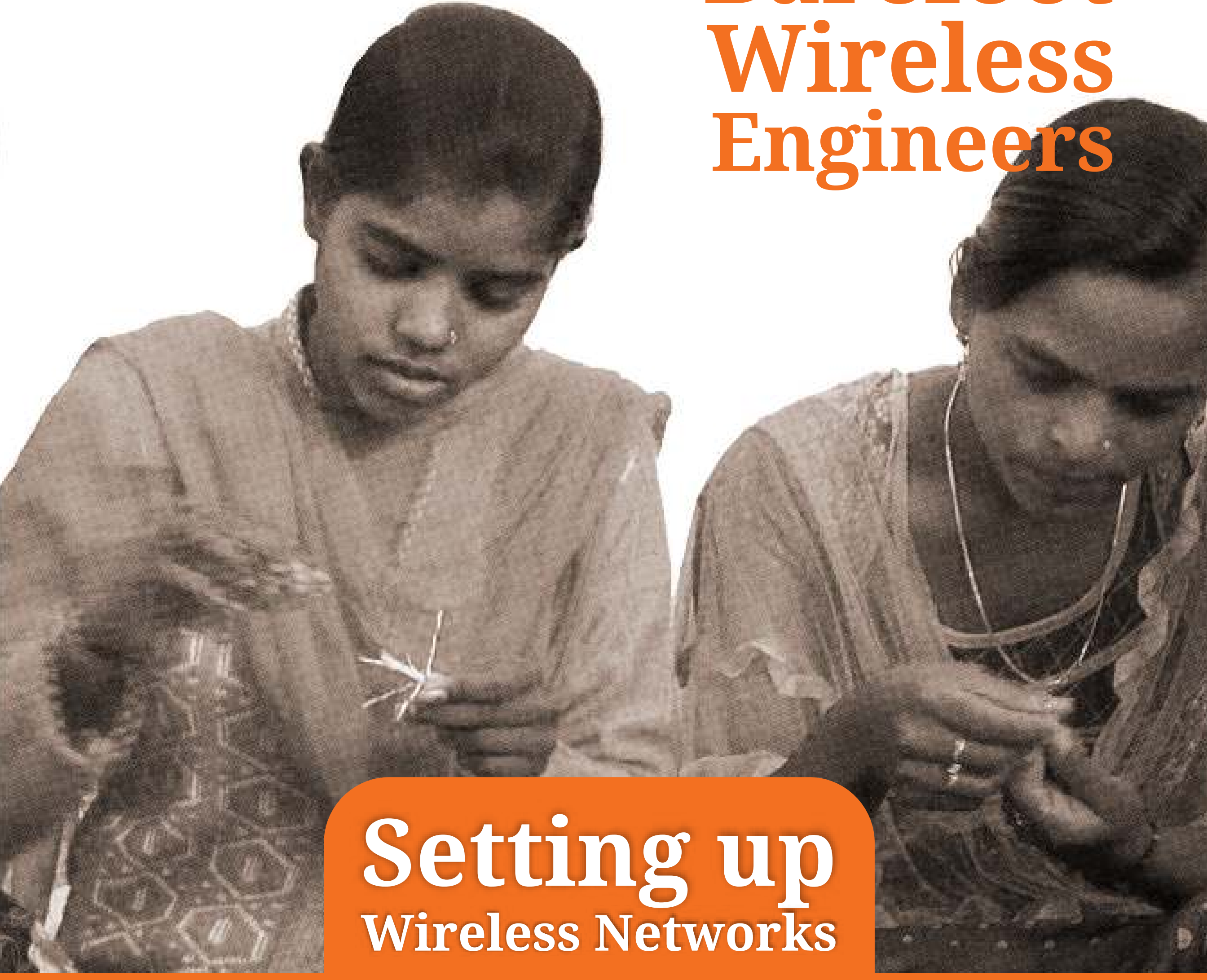
COMMONWEALTH of LEARNING
Learning for Sustainable Development

DEF
DIGITAL EMPOWERMENT foundation

A Course for Barefoot Wireless Engineers



Setting up Wireless Networks

MODULE II

Installation & Maintenance

Copyright

The ‘Barefoot Wireless Engineers’ course has been developed as part of the collaborative advanced ICT course development project of the Commonwealth of Learning (COL). COL is an intergovernmental organisation created by Commonwealth Heads of Government to promote the development and sharing of open learning and distance education knowledge, resources and technologies.

Digital Empowerment Foundation (DEF), established in 2002, aims to connect unreached and underserved communities of India in an effort to bring them out of digital darkness and equip them with access to information. With the belief ‘Inform, Communicate and Empower,’ DEF finds sustainable digital interventions to overcome information poverty in rural and remote locations of India, and empower communities with digital literacy, digital tools and last mile connectivity.

This course is intended to be used and shared freely by trainers working in development and civil society organisations such as telecentres, community media organizations and NGOs.

For the avoidance of doubt, by applying this licence the Commonwealth of Learning does not waive any privileges or immunities from claims that it may be entitled to assert, nor does the Commonwealth of Learning submit itself to the jurisdiction, courts, legal processes or laws of any jurisdiction. The ideas and opinions expressed in this publication are those of the author/s; they are not necessarily those of Commonwealth of Learning and do not commit the organisation.

Course Team

Orginal Content Development: Wireless for Community Team of Digital Empowerment Foundation

Course Outline & Structure: Shahid Ahmad, Ritu Srivastava, CommonWealth of Learning, Madhu Parhar & Vasanta Akondy

Instructional Designer: Vasanta Akondy

Graphic Designer & Illustrator: Ravi Kr. Yadav & Sharada Kerkar

The course has been developed with the support of the Commonwealth of Learning, Canada.

Published by

Digital Empowerment
Foundation
House No 44,
III Floor, Kallu Sarai
Near Narayan Academy,
New Delhi-110017, India

Fax: +91 1126532787

Telephone +91 11 26532787

E-mail: def@defindia.net

Website: www.defindia.org

A COURSE FOR BAREFOOT WIRELESS ENGINEERS

SETTING UP WIRELESS NETWORKS

Module II - Installation & Maintenance

Acknowledgements

The Digital Empowerment Foundation wishes to thank the organizations and individuals mentioned below for their contribution to this Self-Study Handbook:

- Commonwealth of Learning (COL)
- The Internet Society (ISOC)
- Madhu Parhar
- Vasanta Akondy
- Osama Manzar
- Shahid Ahmad
- Ritu Srivastava
- Jazbe Rizvi
- Aamir Rahman
- Fauziya Nasim
- Babloo Das
- Aakash Dhakre
- Layak Ram
- Community members

Table of Contents

About this Self-Study Handbook

Setting up Wireless Networks – A Course for Barefoot Wireless Engineers has been produced by the Digital Empowerment Foundation. This course is divided into two parts. The first part covers some basic concepts related to planning the setup of wireless networks such as conducting a location survey and selecting the required hardware. The second part of the handbook covers details of actual installation and maintenance of wireless networks.

HOW THIS SELF-STUDY HANDBOOK IS STRUCTURED?

The course overview

The course overview gives you a general introduction to the course. The information contained in the course overview will help you determine:

- If the course is suitable for you.
- What you will already need to know.
- What you can expect from the course.
- How much time you will need to invest to complete the course.

The overview also provides guidance on:

- Study skills.
- Where to get help.
- Course assignments and assessments.
- Activity icons.
- Units.

We strongly recommend that you read the overview carefully before starting your study

The course content

The course is broken down into units. Each unit comprises:

- An introduction to the unit content.
- Unit outcomes.
- New terminology.
- The core content of the unit with a variety of learning activities.
- A unit summary.
- Assignments and/or assessments, as applicable

Resources

For those interested in learning more on this subject, we provide you with a list of additional resources at the end of this handbook; these may be books, articles or websites.

Your comments

After completing Setting up Wireless Networks we would appreciate it if you would take a few moments to give us your feedback on any aspect of this course. Your feedback might include comments on:

- Course content and structure.
- Course reading materials and resources.
- Course assignments.
- Course assessments.
- Course duration.
- Course support (assigned tutors, technical help, etc.)

Your constructive feedback will help us to improve and enhance this course.

Course overview

WELCOME TO SETTING UP WIRELESS NETWORKS - A COURSE FOR BAREFOOT WIRELESS ENGINEERS

To bring in last mile connectivity for underserved rural and semi-rural areas in India, line-of-sight wireless connectivity is deployed by using low-cost Wireless equipment and the unlicensed frequency spectrum of 2.4 GHz and 5.8 GHz range to create community-operated wireless networks. To further empower the local community, the community members need to be trained in setting up wireless networks themselves.

To view the corresponding video on the course website, you can scan the QR Code displayed here or directly log in to the course website http://lms.defindia.org

Video Duration: 1:40 Minutes

For the purpose of this course, it is assumed that there are three levels at which learners will set up a wireless network. This course is structured to train community members from processes required for Level 1 implementation to processes for Level 3 implementation.

The three levels are:

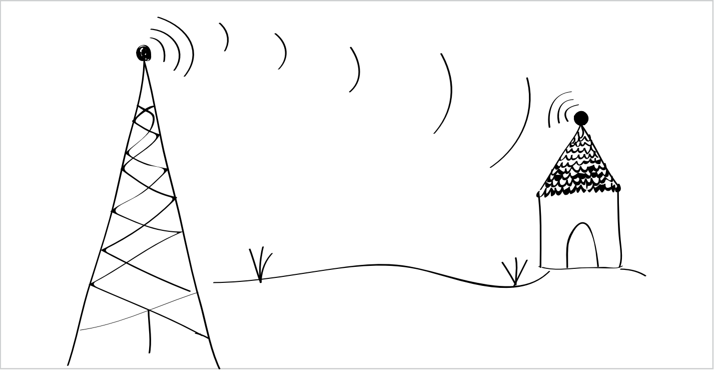


Figure 1 - Level 1, to bring connectivity from the ISP to a single location

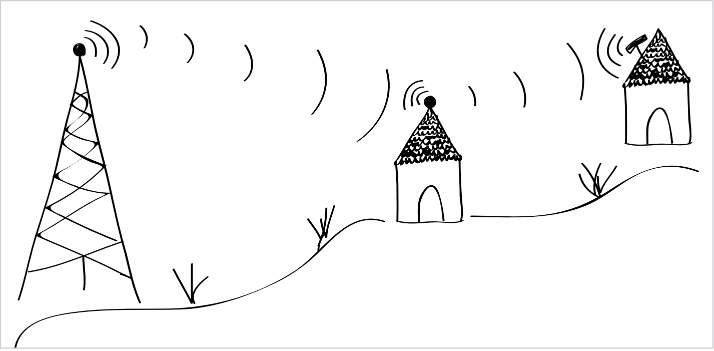


Figure 2 - Level 2, to extend connectivity from the single location to another location

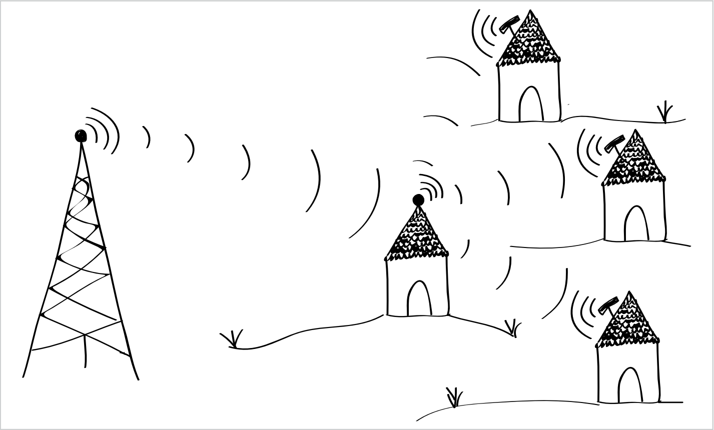


Figure 3 - Level 3, to extend connectivity from the single location to multiple locations

SETTING UP WIRELESS NETWORKS - A COURSE FOR BAREFOOT WIRELESS ENGINEERS — IS THIS COURSE FOR YOU?

This course is intended for community members, especially in rural areas of India, who can set up last-mile Internet connectivity for their communities. These members may not have a formal degree in technical areas such as networking or engineering.

Some of the skills that will help you complete this course are:

- Basic knowledge of English
- Using the Internet for Google search or seeing videos
- Installing apps on a mobile phone
- Using a computer
- Downloading and installing software on a computer
- Understanding of common concepts such as the Internet, network, mobile services etc.

Outomes

COURSE OUTCOMES

Upon completion of Setting up Wireless Networks - A Course for Barefoot Wireless Engineers you will be able to:

- explain the benefits of a wireless network in bringing connectivity to rural areas.
- conduct a location survey before setting up a wireless network.
- determine an optical line-of-sight between two points without interference.
- select equipment that is suitable for the planned wireless network.
- prepare the required agreements and approvals before installing the wireless network.
- install the primary infrastructure for a wireless network.
- install power backup for the wireless network.
- establish maintenance procedures for the wireless network.

Time

TIMEFRAME

What is the expected duration of this course?

60 hours (4 hours per day)

How much formal study time is required?

It is good to have the knowledge of the following

- Basic knowledge of English
- Able to use the Internet for Google search or seeing videos
- Able to install apps on a mobile phone
- Able to use a computer
- Able to download and install software on a computer
- Able to understand the common concepts such as the Internet, network, mobile services etc.

How much self-study time is expected/recommended?

20 hours (4 hours per day)

Study Skills

STUDY SKILLS

As an adult learner, your approach to learning will be different to that from your school days: you will choose what you want to study, you will have professional and/or personal motivation for doing so and you will most likely be fitting your study activities around other professional or domestic responsibilities.

Essentially you will be taking control of your learning environment. As a consequence, you will need to consider performance issues related to time management, goal setting, stress management, etc. Perhaps you will also need to reacquaint yourself in areas such as essay planning, coping with exams and using the web as a learning resource.

Your most significant considerations will be time and space i.e. the time you dedicate to your learning and the environment in which you engage in that learning.

We recommend that you take time now—before starting your self-study—to familiarize yourself with these issues. There are a number of excellent resources on the web. A few suggested links are:

- http://www.how-to-study.com/

The "How to study" web site is dedicated to studying skills resources. You will find links to study preparation (a list of nine essentials for a good study place), taking notes, strategies for reading textbooks, using reference sources, test anxiety.

- http://www.ucc.vt.edu/stdysk/stdyhlp.html

This is the web site of the Virginia Tech, Division of Student Affairs. You will find links to time scheduling (including a "where does time go?" link), a study skill checklist, basic concentration techniques, control of the study environment, note taking, how to read essays for analysis, memory skills ("remembering").

- http://www.howtostudy.org/resources.php

Another "How to study" web site with useful links to time management, efficient reading, questioning/listening/observing skills, getting the most out of doing ("hands-on" learning), memory building, tips for staying motivated, developing a learning plan.

The above links are our suggestions to start you on your way. At the time of writing these web links were active. If you want to look for more go to www.google.com and type "self-study basics", "self-study tips", "self-study skills" or similar.

Help

NEED HELP?

This course is available as a training manual. A companion website for the course is available at the website http://lms.defindia.org. You can log in to the course website using your user ID and password.

The course website can be used to download softcopies of this manual, view corresponding videos, upload assignments and attempt the unit assessment online.

Digital Empowerment Foundation (DEF) will provide additional teaching assistance. It is located in House No 44, III Floor, Kalu Sarai, New Delhi - 110017. Any learner can reach out for any query related this handbook and course at given email defindia@defindia.net.

Assignment

ASSIGNMENTS

At the end of some units, an assignment may be given to help you practice the concepts learned in this course.

The assignments are optional and can be uploaded to the online course for peer feedback and discussion. These assignments are not graded. However, your submissions are visible to other learners and can be used for discussion and feedback. You can also read and comment on assignment submissions made by other learners.

Ideally, you should work on the assignment immediately after completing the corresponding unit. This will help you practice the concepts covered in the unit.

Assessment

ASSESSMENTS

How many assessments will there be in this course?

There are 20 assessments in this course

Are they self-assessments or teacher-marked assessments?

All of the assessments are self-assessments.

When will the assessments take place?

The assessments can be taken by learner as per their learning pace.

How long will the assessments be?

Assessments will take 1 hour and 40 minutes

How long will learners be allowed to complete the assessment(s)?

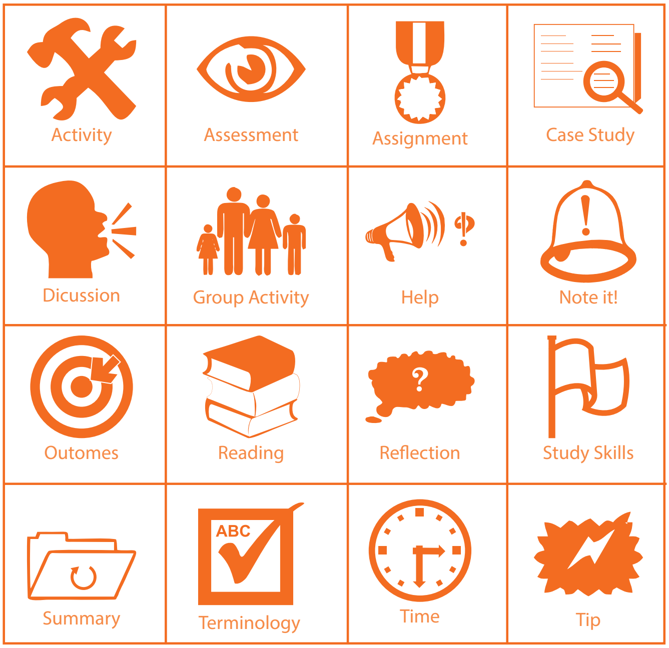
Learners are allowed to take 2 hours to complete the assessments

Getting around this Self-Study Handbook

MARGIN ICONS

While working through this Self-Study Handbook you will notice the frequent use of margin icons. These icons serve to “signpost” a particular piece of text, a new task or change in activity; they have been included to help you to find your way around this Self-Study Handbook.

A complete icon set is shown below. We suggest that you familiarize yourself with the icons and their meaning before starting your study.



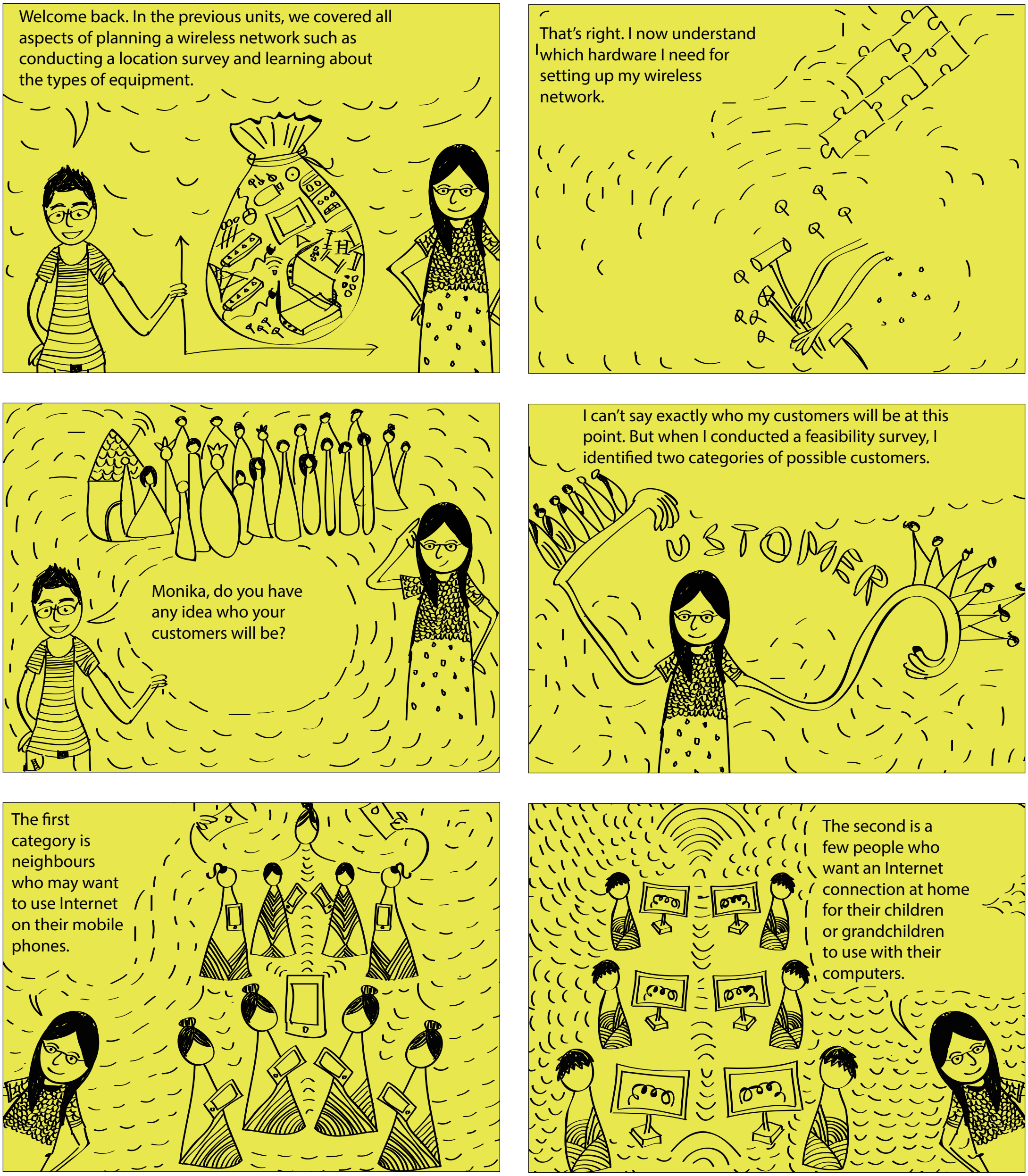
Unit

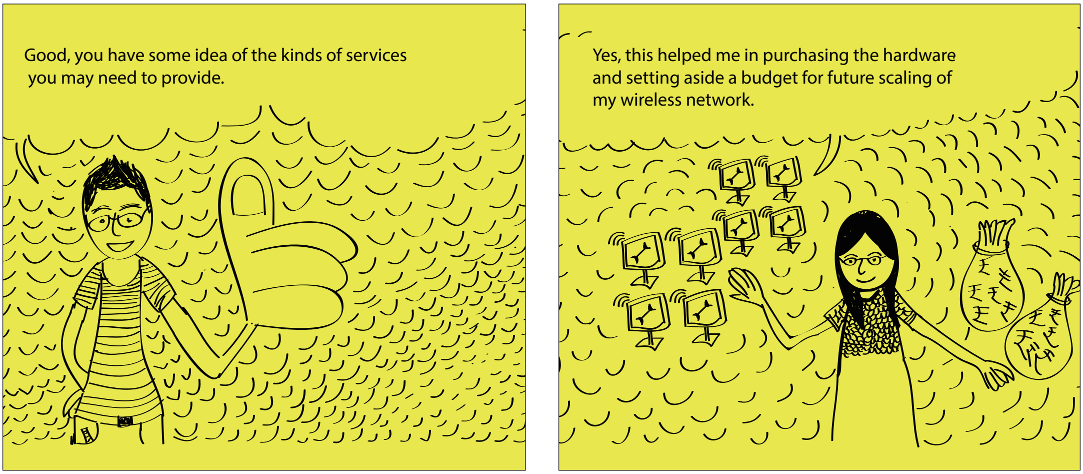
5

Pre-Work before Installation

Introduction

After equipment planning , Monika is now ready to learn pre-work berfore installation.


Welcome back. In the previous units, we covered all aspects of planning a wireless network such as conducting a location survey and learning about the types of equipment.
That's right. I now understand which hardware I need for setting up my wireless network.
Monika, do you have any idea who your customers will be?
I can't say exactly who my customers will be at this point. But when I conducted a feasibility survey, I identified two categories of possible customers.
USTOMER
The first category is neighbours who may want to use Internet on their mobile phones.
The second is a few people who want an Internet connection at home for their children or grandchildren to use with their computers.


Good, you have some idea of the kinds of services you may need to provide.
Yes, this helped me in purchasing the hardware and setting aside a budget for future scaling of my wireless network.

!

To view the corresponding video on the course website, you can scan the QR Code displayed here or directly log in to the course website http://lms.defindia.org

Video Duration: 1:19 Minutes

Outomes

Once all the requirements are ready and equipment has been obtained, some pre-work is required before setting up the wireless network. This unit will provide guidance on the tasks that need to be done as part of the pre-work.

Upon completion of this unit you will be able to:

» List the parameters to be considered before selecting a telecom service provider.
» Apply for the required bandwidth.
» Prepare relevant documents such as the ISP franchise agreement, Vendor quotations etc.

Terminology

Backhaul Connectivity: Wireless backhaul is the use of wireless communications systems to get data from an end user to a node in a major network such as the Internet or the proprietary network of a large business, academic institution or government agency

Bandwidth: Bandwidth is the capacity of a wired or wireless network communications link to transmit the maximum amount of data from one point to another over a computer network or internet connection in a given amount of time -- usually one second

Selecting a Service Provider

When a farmer needs water for the fields, he may use a borewell as the source of water. But if he had several borewells to choose from, which borewell would he choose? Based on his requirements, he may choose the nearest one or the one with the most water pressure or one which costs him less (figure 1).

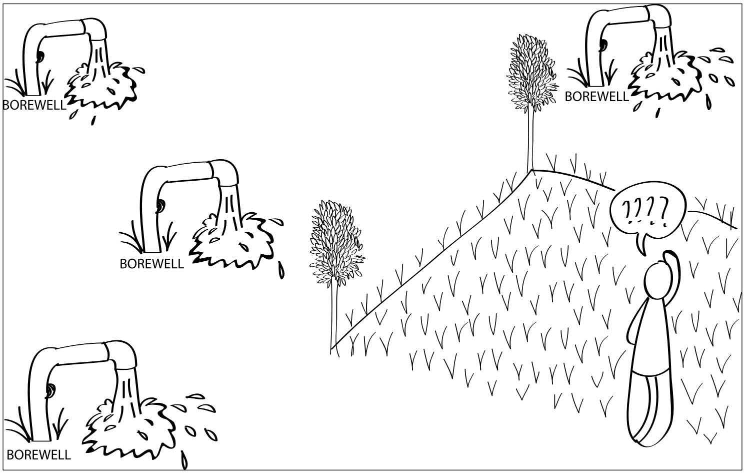
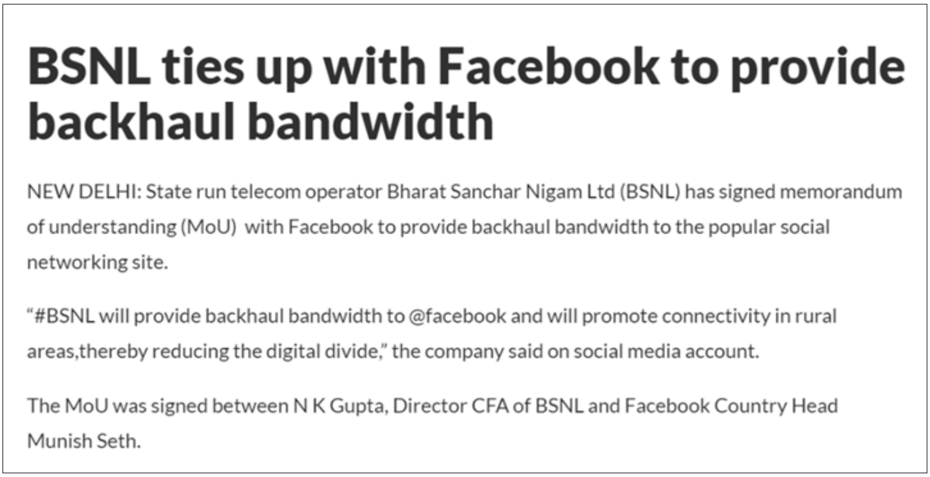


Figure 1. Example of borewell to show the setting up of wireless network

In the same way, when setting up a wireless network you have to decide what your source of the connection is going to be. There are telecom service providers such as BSNL, Airtel etc. from where you can buy the required connection. Based on your requirements, you will have to select a service provider which suits your needs best. When getting bandwidth for the purpose of connecting smaller networks with the backbone or a primary network such as BSNL, it is known as backhaul bandwidth or backhaul connectivity.



BSNL ties up with Facebook to provide backhaul bandwidth

NEW DELHI: State run telecom operator Bharat Sanchar Nigam Ltd (BSNL) has signed memorandum of understanding (MoU) with Facebook to provide backhaul bandwidth to the popular social networking site.

"#BSNL will provide backhaul bandwidth to @facebook and will promote connectivity in rural areas,thereby reducing the digital divide," the company said on social media account.

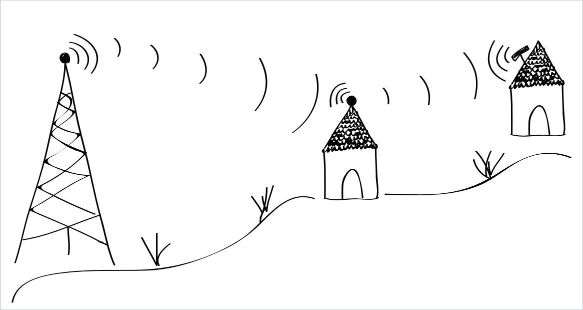
The MoU was signed between N K Gupta, Director CFA of BSNL and Facebook Country Head Munish Seth.

Figure 2 - Example of backhaul bandwidth

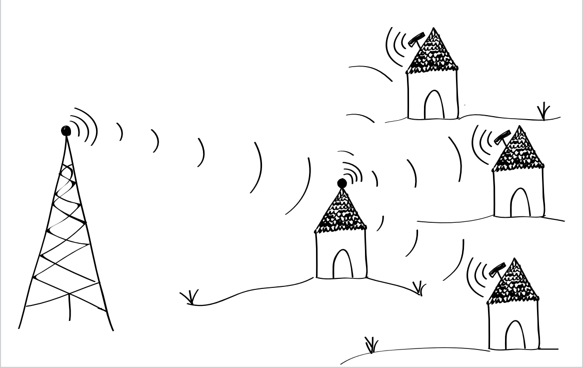
Consider Monika's case. She is likely to have customers who will need an Internet connection at home. That means, she should have enough Internet bandwidth at her centre which can further be distributed. So she needs to select a service provider who can give her the required bandwidth. What are some of the other considerations when selecting a telecom service provider?

The main consideration is the purpose of the wireless connection – whether it is for Level 1 connectivity or Level 2 or Level 3 connectivity (figure 3).

Level 1, to bring connectivity from the ISP to a single location



Level 2, to extend connectivity from the single location to another location



Level 3, to extend connectivity from the single location to multiple locations

Figure 3 - Levels of connectivity

If you are only looking at a level 1 internet connectivity, you can aim to get a bandwidth of speed 2 Mbps. However, if you are looking at distributing the internet at level 2 or level 3 connectivity, you can aim to get 2 to 4 Mbps bandwidth which can be increased later as your clients increase.

The next step is to identify all the service providers close to your locality which can provide you with the required bandwidth at your location. Make a list of the service providers. Once this is done, you need to compare the service providers so that you identify the most suitable provider for your specific requirements.

Here is a sample checklist that you can use to compare the various service providers.

If you are only looking at a level 1 internet connectivity, you can aim to get a bandwidth of speed 2 Mbps. However, if you are looking at distributing the internet at level 2 or level 3 connectivity, you can aim to get 2 to 4 Mbps bandwidth which can be increased later as your clients increase.

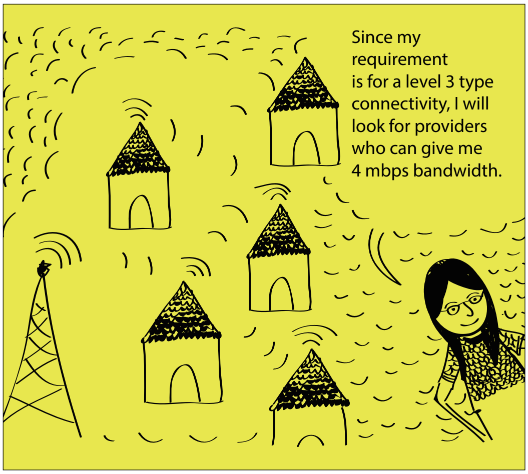
The next step is to identify all the service providers close to your locality which can provide you with the required bandwidth at your location. Make a list of the service providers. Once this is done, you need to compare the service providers so that you identify the most suitable provider for your specific requirements.

Here is a sample checklist that you can use to compare the various service providers.

Table 1: Sample checklist to comapre the various service rproviders

	Service	Service Provider 1	Service Provider 2
1.	What are the bandwidth speeds provided?		
2.	What are the monthly data consumption limits?		
3.	Are there any limits to the file sizes that can be uploaded or downloaded?		
4.	What is the reputation of this service provider when it comes to speed and reliability?		
5.	Will the service provider allow installation of your devices in their base station?		
6.	What kind of power backup does the service provider offer?		
7.	What is the cost of the bandwidth?		
8.	Are the charges a flat rate or are they metered based on the choice of bandwidth consumption?		
9.	Are there any hidden costs such as for additional hardware, installation or power backup?		
10.	Does this provider have a vendor contract or a service level agreement?		
11.	What is the minimum contract duration or lock-in period?		
12.	What kind of support will this provider give during the contract period?		
13.	What security measures does this provider give to protect your network from viruses, malware and hacking?		

1
2
3
4
5
6
7
8
9
10
11
12
13
Great, I can use this checklist to identify which service provider I can use.


Since my requirement is for a level 3 type connectivity, I will look for providers who can give me 4 mbps bandwidth.

Here is a sample plan that could suit the kind of requirements Monika has.

Table 2: Sample plan for identifying bandwidth

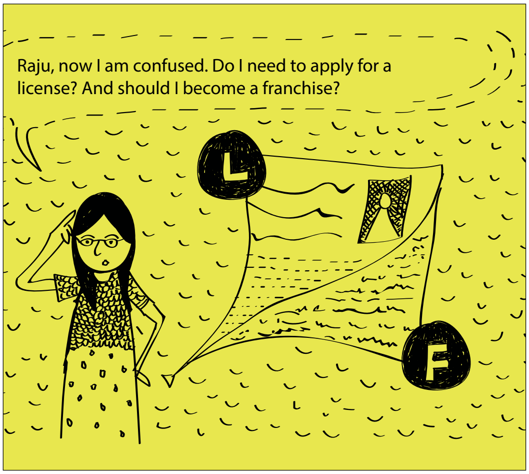
Bandwidth (Download Speed) subject to technical feasibility	up to 4 Mbps
Monthly Charges (Rs)	150
Annual Payment Option (Rs) [11 x FMC]	1650
Two Years Payment Option (Rs) [21 x FMC]	3150
Three Years Payment Option (Rs) [30 x FMC]	4500
Download/Upload Limit (MB/ GB) per month	1 GB
Additional Usage Charges/MB beyond free download/upload limit (Rs)	0.30 upto 3 GB, 0.10 Beyond 3 GB
Night Unlimited (0200-0800 Hrs)	No
Free E-mail IDs/Space (Per E-mail ID)	1/1 GB
Security Deposit	Nil
Minimum Hire Period	Nil
Committed Period for FREE MODEM	Nil
Type of Modem	ADSL Basic

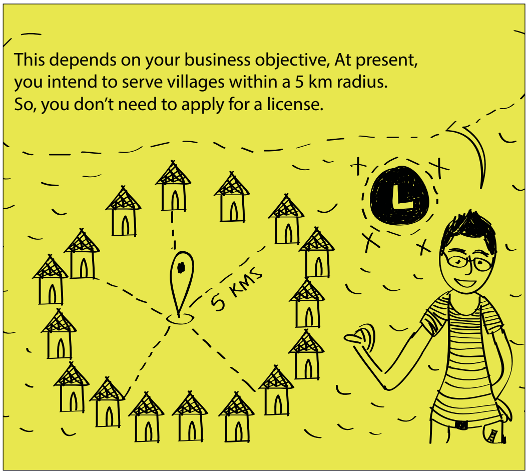
Applying for Bandwidth with License

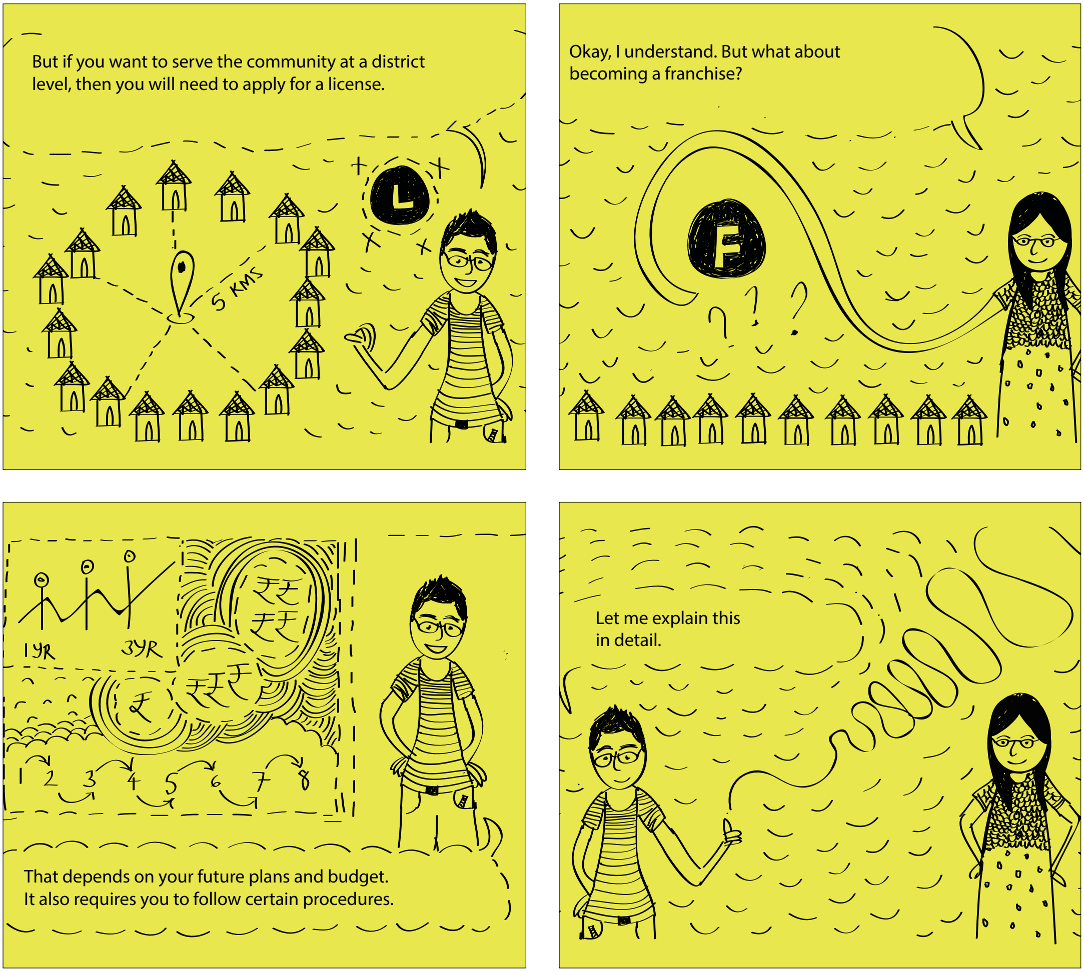
Telecom service providers are governed by the laws and regulations of the country in which they operate. In India, the government issues these service providers a license to distribute internet bandwidth. There are three main kinds of license circles:

- Level (National)
- Level (State)
- Level (District)

Private entities such as Vodafone, Airtel or idea apply for a license to distribute the internet connectivity as per the license circle of their business operations. However, there are other mechanisms to distribute internet bandwidth. For example, small-sized providers may become a franchise of the main ISP provider and distribute it further. Or, small-sized providers can apply for Virtual Network Operator (VNO) license to distribute the network at a smaller scale (multiple block level).


Raju, now I am confused. Do I need to apply for a license? And should I become a franchise?
L
F


This depends on your business objective, At present, you intend to serve villages within a 5 km radius. So, you don't need to apply for a license.
5 KMS
L


But if you want to serve the community at a district level, then you will need to apply for a license.
5 KMS
L
Okay, I understand. But what about becoming a franchise?
F
? ? ?
1YR
3YR
₹₹
₹₹
₹₹₹
₹
1 2 3 4 5 6 7 8
That depends on your future plans and budget. It also requires you to follow certain procedures.
Let me explain this in detail.

But to become a wireless network entrepreneur, you can become a franchise of the main ISP provider and serve the community.

To become a franchise, you buy bulk bandwidth from an ISP and distribute it. For example, Monika could buy bulk bandwidth from BSNL and distribute it to other users either through a wireless network or through a wired network. A franchise is required to adhere to the ISP's guidelines and maintain data such as user logs, complaint logs and equipment status. This is applicable when operating at a village, block or a small scale. In this case, a license is not required. A franchise can operate under any brand name.

A non-franchise service is like any other internet provider which needs to obtain a license from the government - either national, state or district level or VNO level as applicable. Refer to the appendix for details.

Reading

ADDITIONAL READING

Regulatory Environment in India (Page 24)

http://defindia.org/wp-content/uploads/2017/09/Community-Networks-Regulatory-Issues-Gaps.pdf

VNO license

http://dot.gov.in/sites/default/files/2016_07_05%20VNO-AS-I.pdf?download=1

Summary

UNIT SUMMARY

In this unit, you learned about the parameters to be considered before selecting a telecom service provider. You also learned about the different license circles in India. Finally, you learned about being a franchise of an ISP.

Assignment

ASSIGNMENT

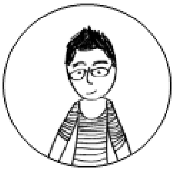
Your Vendor Comparison

Assume that you are going to select a bandwidth plan for your centre. Select any two service providers such as BSNL/MTNL, Airtel, Vodafone etc. in your location and fill the comparison list given in this unit. You can visit the service providers' websites or their local offices to get the required information.

This assignment is for your practice and need not be uploaded to the course website.

Assessment

ASSESSMENT



Now that you have completed this unit, check your understanding of the concepts learned by responding to the following questions.

You can also take this assessment on the course website.

You can compare your response with the response displayed in the Ideal Responses section.

Question 1: Vijay is looking at setting up an Internet browsing centre at his house with four computers. He intends to try this for one year and then decide if he should increase the number of computers in his centre. What is the ideal Internet speed he should select?

a. up to 1 Mbps
b. up to 2 Mbps
c. up to 4 Mbps
d. up to 8 Mbps

Question 2: If you are providing services at a district level, you don't need a license. Is it true or false?

a. True
b. False

IDEAL RESPONSES

Answer 1: b. For using the internet with four computers, a bandwidth of up to 2 Mbps is sufficient. It may not be advisable to spend more for higher bandwidth at the beginning.

Answer 2: b. A license is required for providing services at a district level. A C level license circle is applicable in such a scenario.

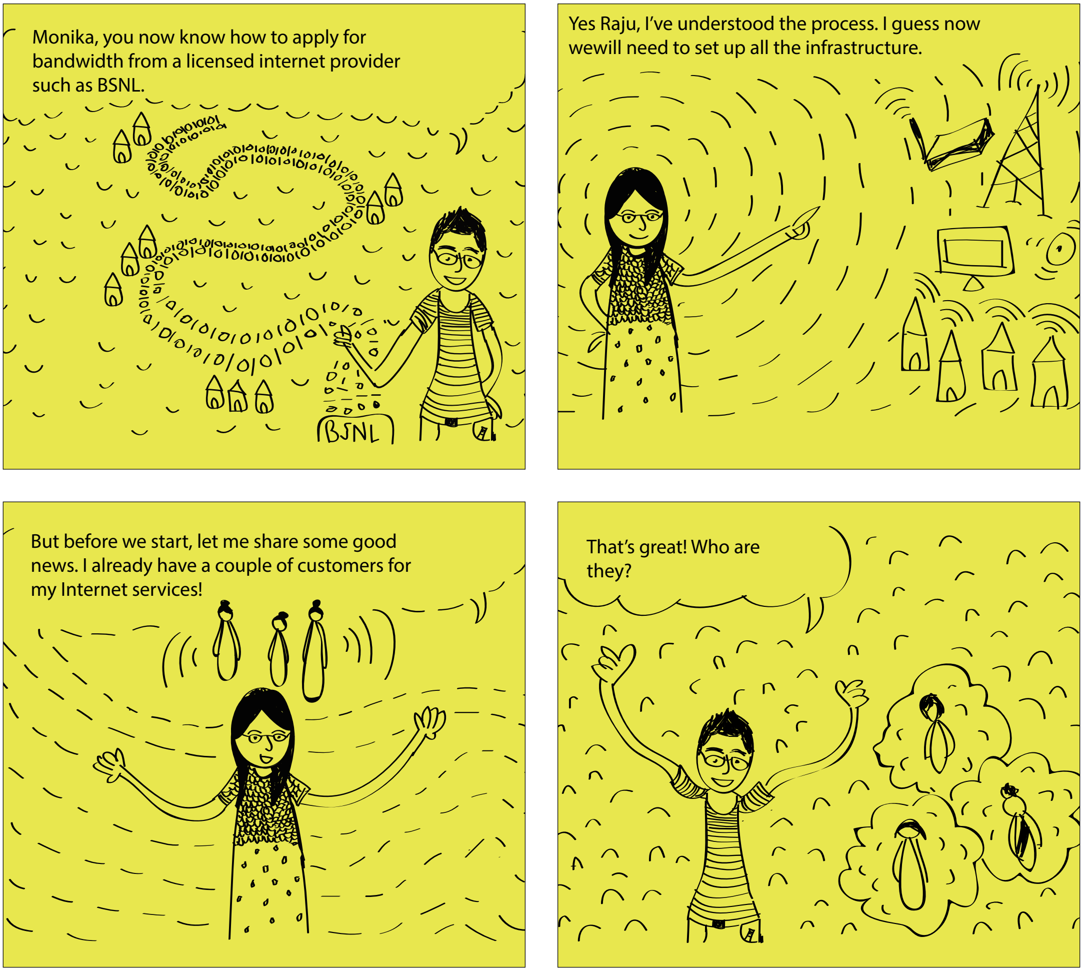
Unit

6

Primary Infrastructure Setup

Introduction

Read the story of Monika who is now ready to set up primary infrastructure for the wireless network.


Monika, you now know how to apply for bandwidth from a licensed internet provider such as BSNL.
BSNL
Yes Raju, I've understood the process. I guess now wewill need to set up all the infrastructure.
But before we start, let me share some good news. I already have a couple of customers for my Internet services!
That's great! Who are they?

The first is my neighbour's daughter. She wants to use Wi-Fi on her mobile phone. She is preparing for competitive exams so she wants to use the Internet for her studies.
100 mt
And the second one is Kabir chacha from our neighbouring village. He wants to monitor his godown from his home, so he wants to set up a wireless camera. He also wants to use the Internet at home to check it.
This is exciting. Looks like one customer is close to your house while the other is at a distance.
So, if you set up a wireless network at your house, then you can provide the Internet connection to your neighbour via a hotspot. So, the infrastructure at your house is the primary infrastructure.

Outomes

Once the bandwidth is available from a telecom service provider or a licensed internet service provider (ISP), you need to set up the infrastructure at the location from where you want to provide the internet services. This unit will cover the details of setting up a wireless network based on all the requirements gathered.

Upon completion of this unit you will be able to:

» List the steps for setting up primary broadcasting infrastructure.

» Set up earthing for broadcasting infrastructure.

» Construct the tower and organise the hardware

ABC

Terminology

Broadcasting A method of transferring a message to all recipients simultaneously.

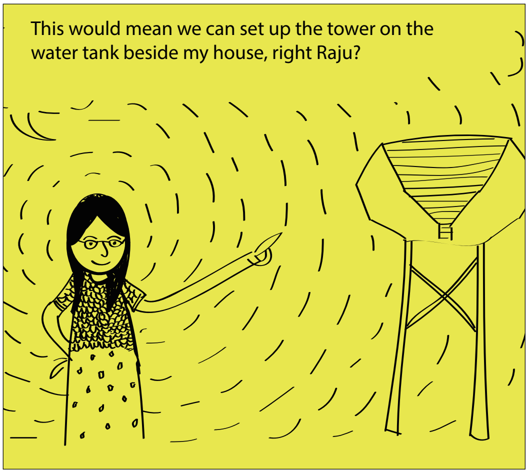
Server In computing, a server is a computer program or a device that provides functionality for other programs or devices, called "clients".

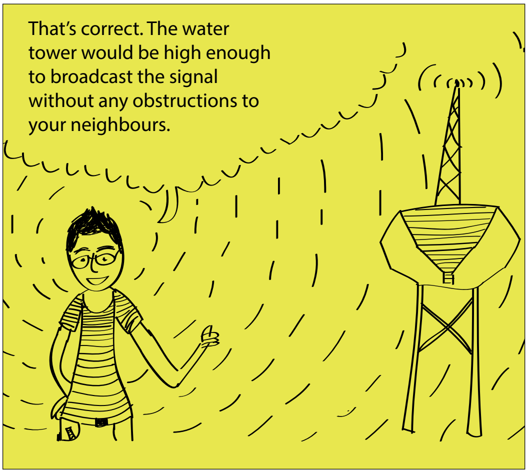
Earthing Also known as bonding or grounding, involves providing a safe path for the current to flow to the Earth in case of a fault during lightening.

Setting up the Tower

In Unit 2, you learned about establishing the line of sight between two locations. In Unit 4 you learned about towers and the kinds of arrangements required for single-user-setup and for a single-to-multipoint setup.

In this unit, you will learn about setting up a tower and the primary infrastructure at the selected location. For the purpose of this example, we will set up a 10-feet tower on the rooftop of the tallest building from where we are broadcasting the internet.


This would mean we can set up the tower on the water tank beside my house, right Raju?


That's correct. The water tower would be high enough to broadcast the signal without any obstructions to your neighbours.

To build the tower, we can use three pipes each of which is 10 feet long. We weld these three pipes together as shown in the figure 4.

As far as the availability of the internet is concerned, there may be two possibilities:

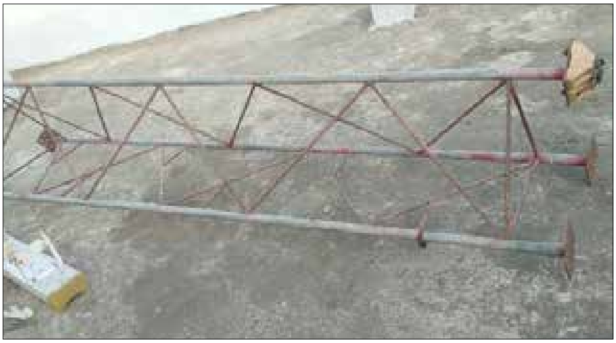


Figure 4 Example of showing 10 feet long tower using three pipes

1. The telecom provider or ISP has provided the internet connectivity at your location.
2. The ISP has not provided internet at your location and you are bringing the connectivity from the base station to the location where you want to set-up the wireless network.

Setting up the primary infrastructure if ISP has provided internet connectivity at your location

Once you establish the tower at the location, establish and set up the transmitter. For example, if we are transmitting the internet in three locations, then three transmitters need to be installed. The configuration of the transmitter will be explained in this unit later on.

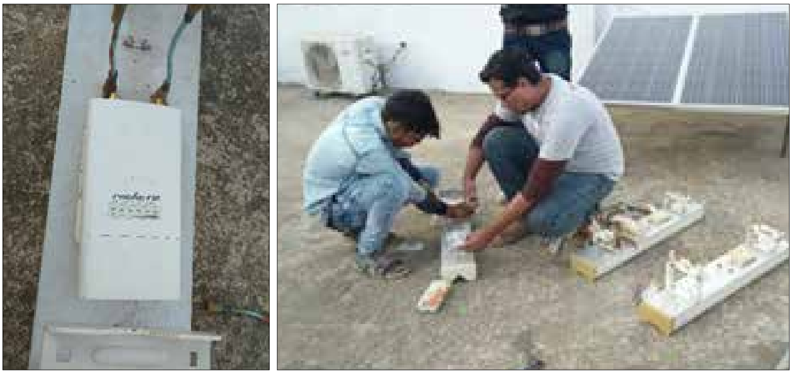


Figure 5: Setting up the transmitter on the tower

Setting up the primary infrastructure if ISP has not provided the internet at your location and you are bringing the connectivity from the base station

In this situation, we need to configure the access-point at the base station of the ISP. The configuration of the access point will be described later in this unit. We also need to set-up the 10-feet tower as described and configure three transmitters. Additionally, one receiver also needs to be set up (fig. 6).

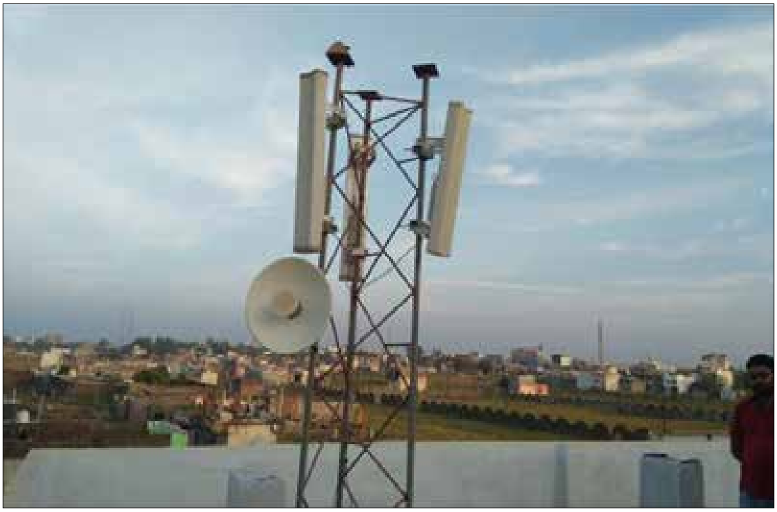


Figure 6 - Tower with three transmitters and one receiver

Before you set-up the devices on the tower-like structure, it is suggested that you configure the devices as per your need. For example, when setting up the transmitters and the receiver displayed in Figure 6, the devices had been configured before they were established on the tower. This is practical because the devices need to be connected to a computer in order to configure them. Since the devices may be mounted at a height or at an odd location, it may be inconvenient to connect them to a computer after installation.

So, the first step is to configure the devices used in the primary infrastructure. A device of any brand such as Microtik or Ubiquity can be used as long as it meets the required specifications.

Note: For configuration, it is important that you know some basics of networking concepts such as IP address, DNS etc. You can also

Figure 7: Server

request someone who knows computer networking to help you with this process. Refer to the Additional Reading section for some learning resources on networking concepts.

For establishing a wireless network from one point to many points, a network needs to be created. This can be done by setting up a router at the server space used for hosting information about the customers. The server is like ledger file where we keep our records and totalling of economic transactions.

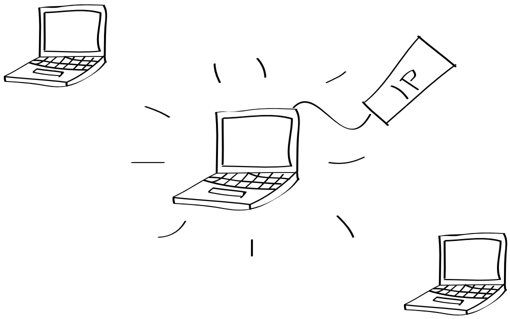
Configuring the Hardware

Once the hardware is purchased, each of the devices needs to be configured. In simple words, configuring means to select the required settings for each device. It's like selecting a ringtone for your mobile phone or tuning a radio station.

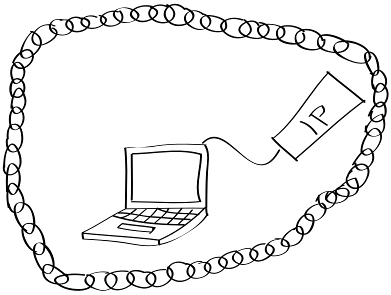
For each device, configuration involves five broad steps.

1. Assign IP
2. Secure the device
3. Create connections
4. Test the device
5. Change configuration

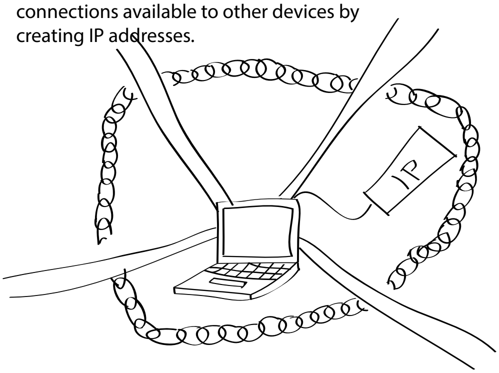
1. Assign IP: Giving the device a unique identity – assigning it an IP address.



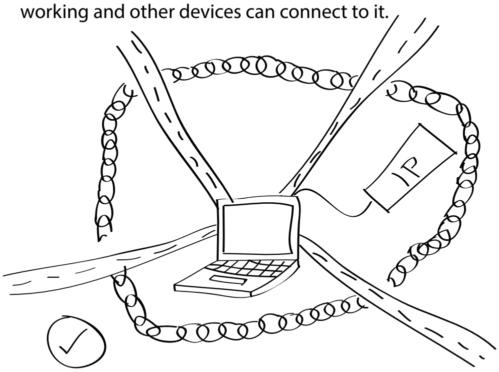
2. Secure the device: Making the device secure so that no one but you can access it.



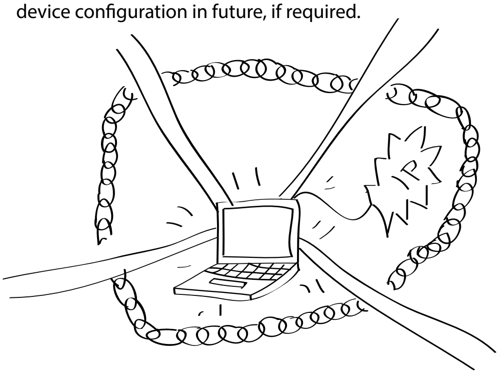
3. Create connections: Then, to make connections available to other devices by creating IP addresses.



4. Test the device: Testing whether the device is working and other devices can connect to it.



5. Change configuration: Making changes to the device configuration in future, if required.



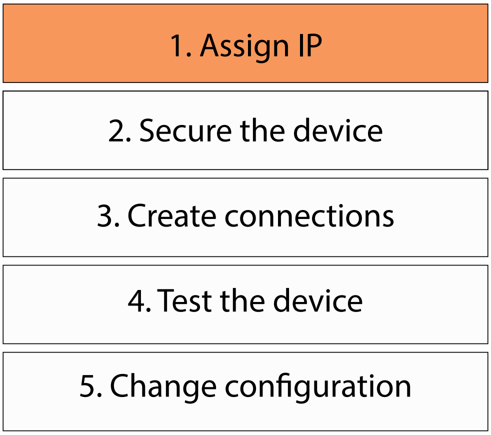
As mentioned briefly, when setting up a wireless network service for multiple customers, you will need to create a personal network. That means, in addition to transmitters and receivers, you will need to install a router. A router allows you to create your own network, manage clients, secure the network and distribute bandwidth. You have already learned about routers in the unit on types of equipment.

Let us first look at the steps for configuring a Microtik router. If you are using another router, you may refer to the configuration steps that are included in the device documentation.

Recall the five broad steps for configuring a device. We will look at the details involved in each of these.

Configuring the Microtik Router using Winbox Software

Let's start with assigning the IP address to the router. For a Microtik router, the configuration has to be done using a software called Winbox. The software helps us 'talk' to the hardware device. This is somewhat like the remote control that helps us 'talk' to the T.V. Winbox can be downloaded from the Microtik website and installed.



1. Assign IP

2. Secure the device

3. Create connections

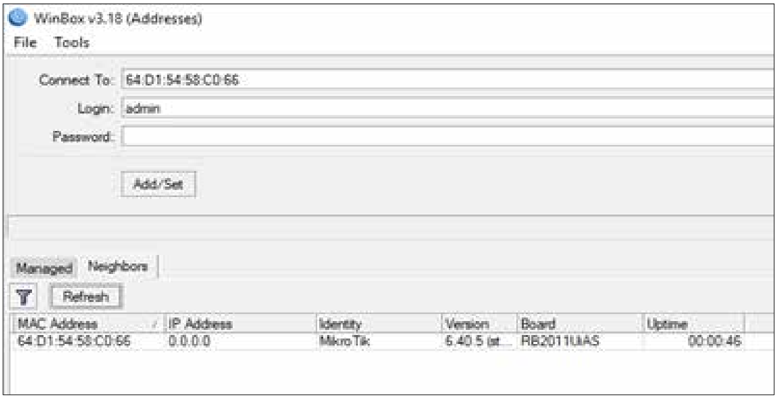
4. Test the device

5. Change configuration

1. Assigning IP to the router

Note: The complete process described below is for a layperson without any knowledge of networking. If you follow these steps accurately, you can create your own network.

1.1. Open the Winbox application and log in. The following screen is displayed. Click on Neighbors > MAC Address of the router in the list.



WinBox v3.18 (Addresses)

Connect To: 64:D1:54:58:C0:66

Login: admin

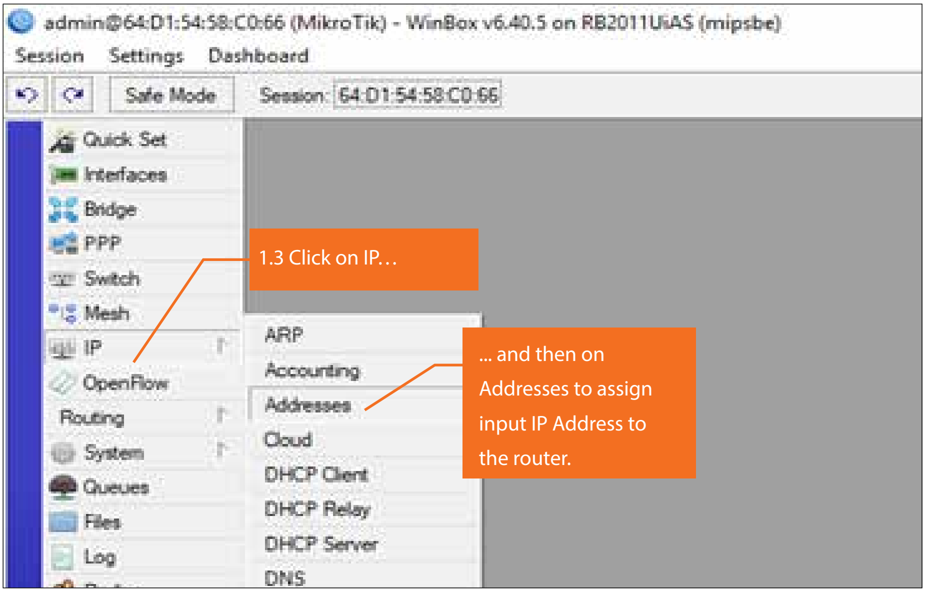
Password:

MAC Address	IP Address	Identity	Version	Board	Uptime
64:D1:54:58:C0:66	0.0.0.0	MikroTik	6.40.5 (st...	RB2011UiAS	00:00:46

WinBox automatically displays the MAC address of the router. In this example, the MAC address of the router and IP address are displayed as 0.0.0.0 because these values have not yet been assigned. Details such as Identity, Version, Board and Uptime are also displayed automatically.

1.1. Click on Connect.

1.2. Click on IP > Addresses.



admin@64:D1:54:58:C0:66 (MikroTik) - WinBox v6.40.5 on RB2011UiAS (mipsbe)

Session: 64:D1:54:58:C0:66

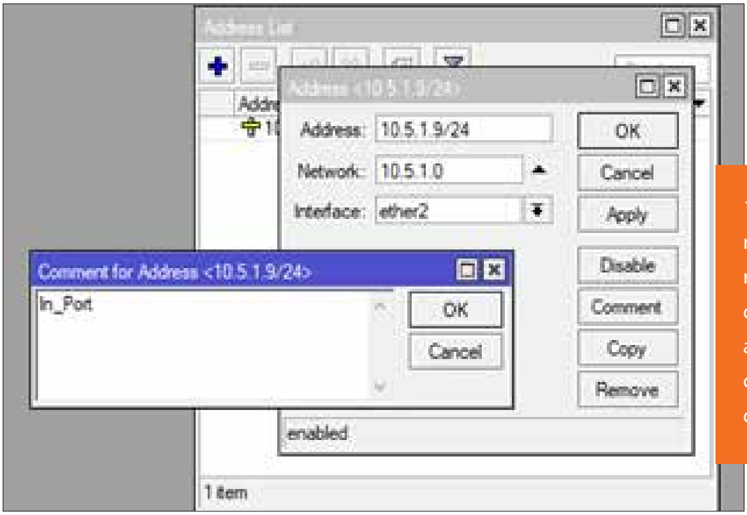
1.3 Click on IP…

... and then on Addresses to assign input IP Address to the router.

The ISP provides you with a set of IP addresses when you apply for a connection. You can think of it as a house number given to your house so that your house can be uniquely identified. So, the electricity board supplies electricity to one point to this unique house number. You can then distribute the electricity to other areas of the house from this point.

The IP address is a set of numbers separated by a dot. We will use Winbox to assign the IP address to the router. We can then distribute data from this router to others in the network.

1.4 Assign the IP address and select the input interface and then click on Apply.



Address: 10.5.1.9/24
Network: 10.5.1.0
Interface: ether2
In_Port
enabled

1.5 To add comments for further reference click on Comment, add the required comments and click on OK.

In the value of the Address, 10.5.1.9/24:

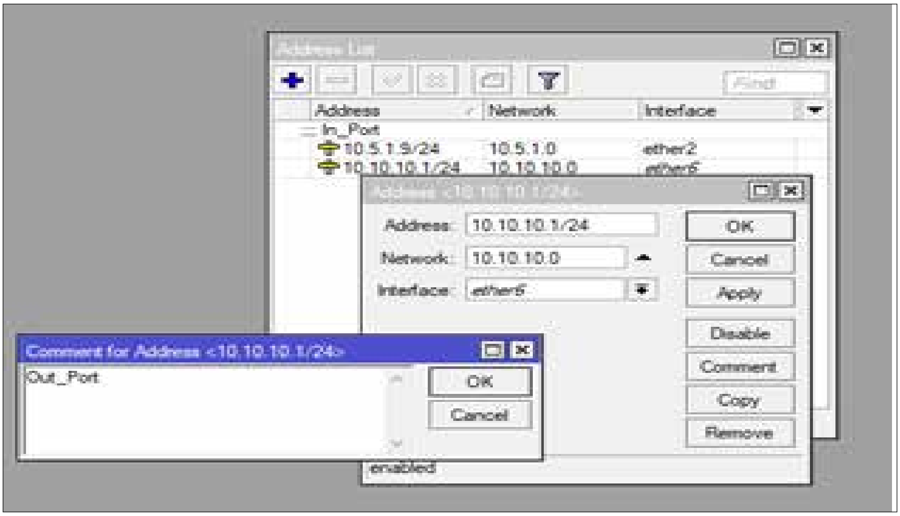
10 - Shows that the bandwidth is from Class A (as explained in Unit 5).

9/24 – Shows that the network is layered from Class A to Class C. This makes it possible to distribute it at a small scale.

The Interface value 'Ether 2' defines the computer to which this router is assigned.

Note: Refer to the appendix for details of IP address classes. You can learn the details of setting up an IP address from the book 'Wireless networking in the developing world', page 116- 140.

1.5 Similarly, assign a local IP address for the internal network and add a comment.



Address	Network	Interface
In_Port		
10.5.1.9/24	10.5.1.0	ether2
10.10.10.1/24	10.10.10.0	ether5

Address <10.10.10.1/24>

Address: 10.10.10.1/24

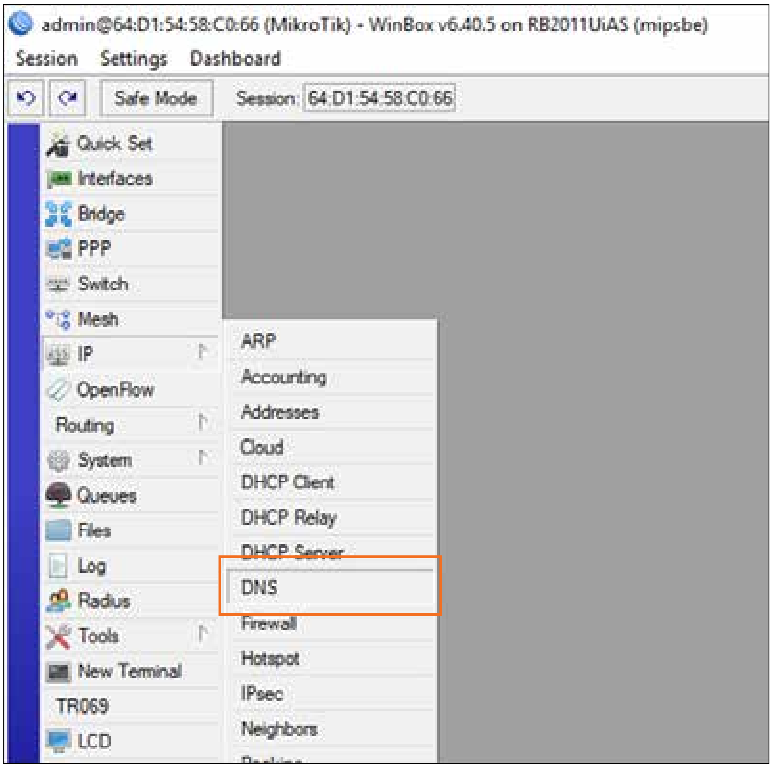
Network: 10.10.10.0

Interface: ether5

enabled

Out_Port

1.6 Click on IP > DNS to assign the DNS.

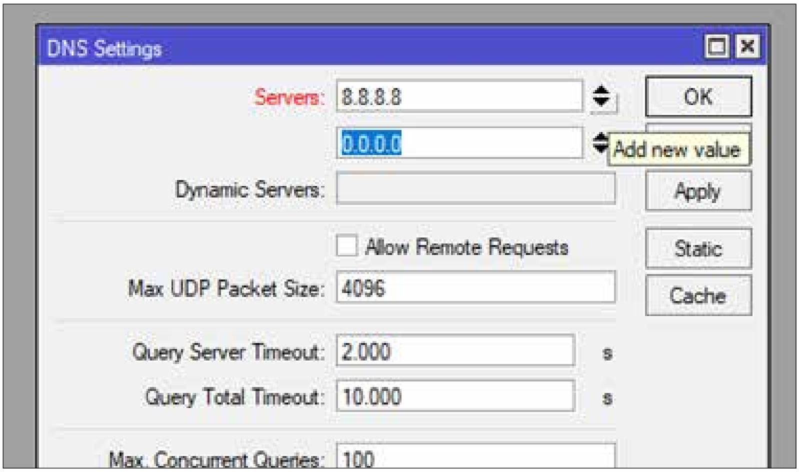


Session: 64:D1:54:58:C0:66

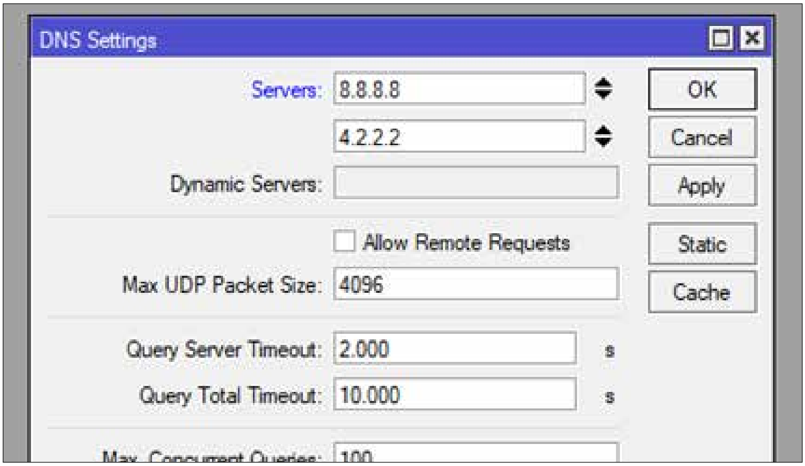
1.7 Type Primary DNS and then Secondary DNS if available. Domain Name System (DNS) is the phonebook of the internet. To store contacts, we need storage. We need both primary and secondary servers. IP Google provides a free DNS service for public use at the IP addresses under IPv4. The primary server is 0.0.0.0 and the secondary server is 4.2.2.2.

Note: You can learn about setting up DNS from the book, 'Wireless networking in the developing world', page 243 – 246. You can learn about Google DNS at

https://en.wikipedia.org/wiki/Google_Public_DNS


DNS Settings

Servers: 8.8.8.8
0.0.0.0
Dynamic Servers:
□ Allow Remote Requests
Max UDP Packet Size: 4096
Query Server Timeout: 2.000 s
Query Total Timeout: 10.000 s
Max. Concurrent Queries: 100


DNS Settings

Servers: 8.8.8.8
4.2.2.2
Dynamic Servers:
□ Allow Remote Requests
Max UDP Packet Size: 4096
Query Server Timeout: 2.000 s
Query Total Timeout: 10.000 s
Max. Concurrent Queries: 100

You have completed the steps for assigning the IP address to the router.

2. Secure the router

1. Assign IP

2. Secure the device

3. Create connections

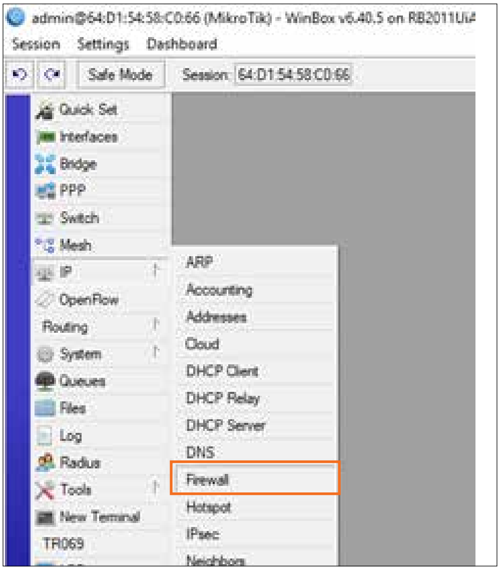
4. Test the device

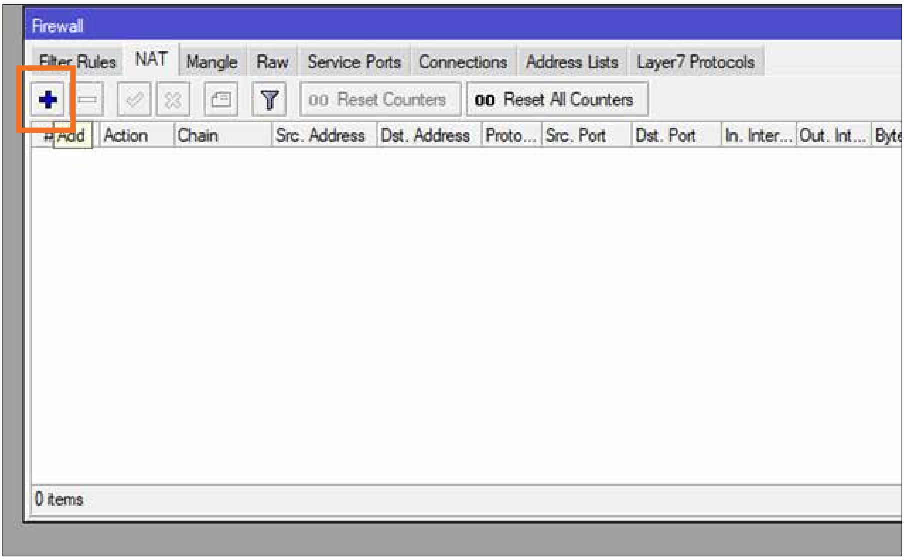
5. Change configuration

The next step is to make sure the router is secure and cannot be accessed without your permission.

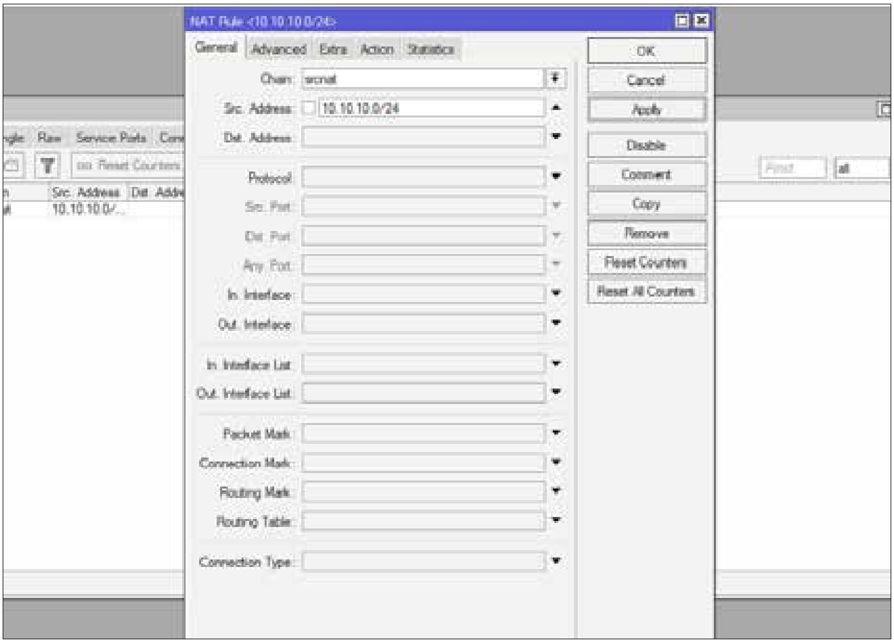
2.1 We will first need to hide or masquerade the network. IP masquerading is a technique that hides an entire IP address space, usually consisting of private IP addresses, behind a single IP address in another, usually public address space.

To masquerade the private network click on IP> Firewall > NAT.



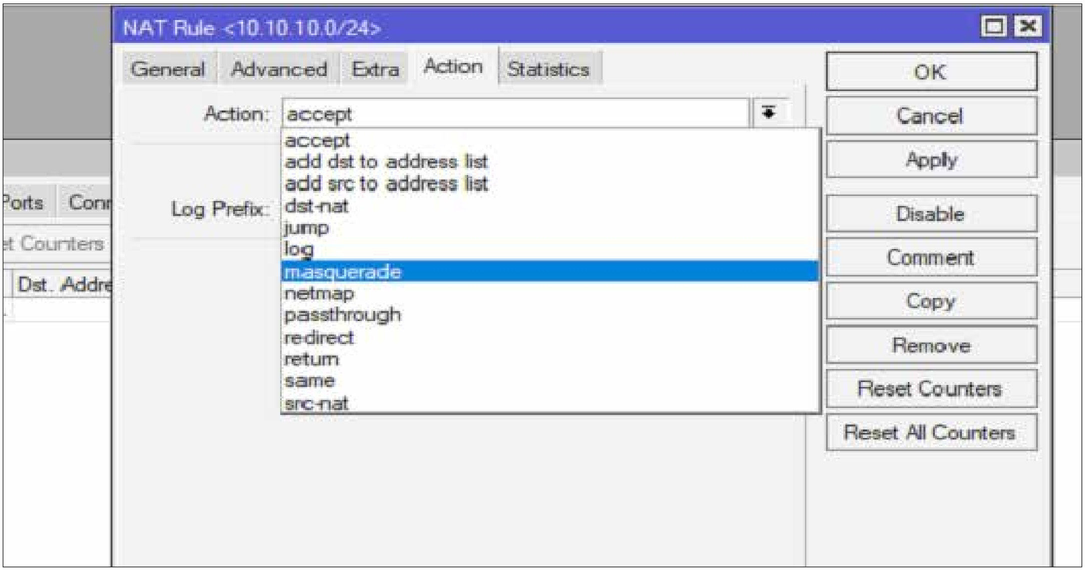


2.2 Click on chain (srcnat) and type the local network address space in Src Address. Click on Action and then click on Masquerade > OK

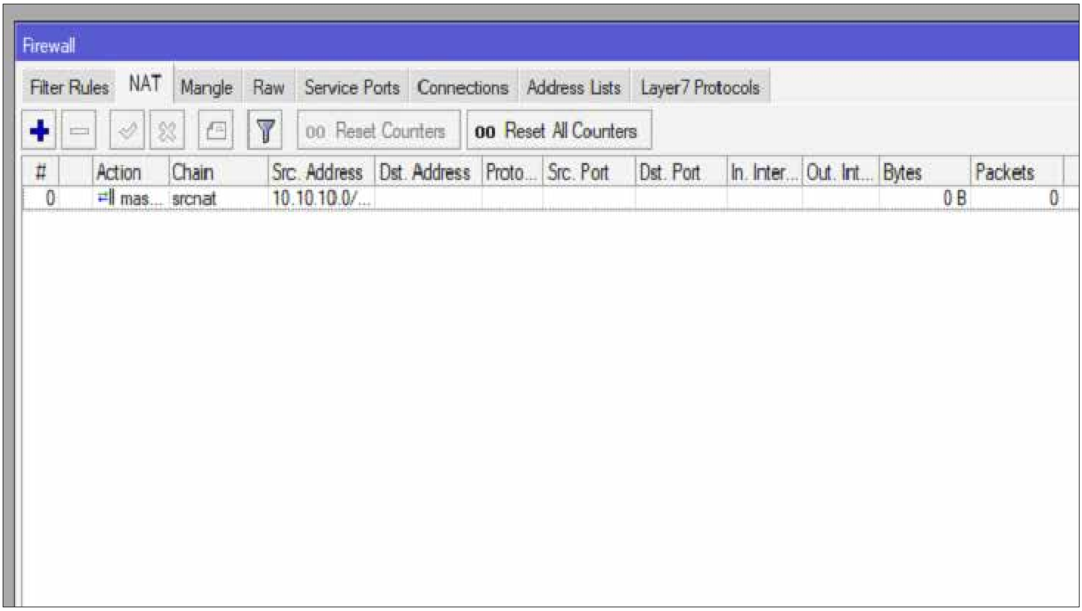

NAT Rule <10.10.10.0/24>

Chain: srcnat

Src. Address: 10.10.10.0/24



Action: accept



#	Action	Chain	Src. Address	Dst. Address	Proto...	Src. Port	Dst. Port	In. Inter...	Out. Int...	Bytes	Packets
0	⇄ mas...	srcnat	10.10.10.0/...							0 B	0

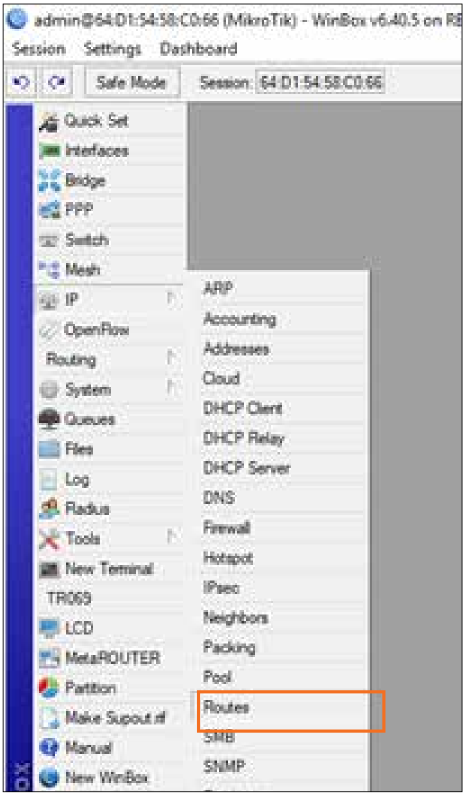
The router is now secure.

3. Create connections

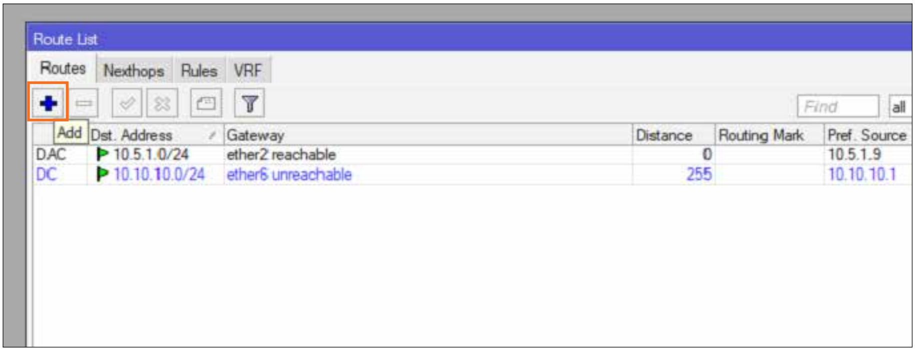
Now, let’s look at the steps for allowing other devices to connect to the router.

1. Assign IP
2. Secure the device
3. Create connections
4. Test the device
5. Change configuration

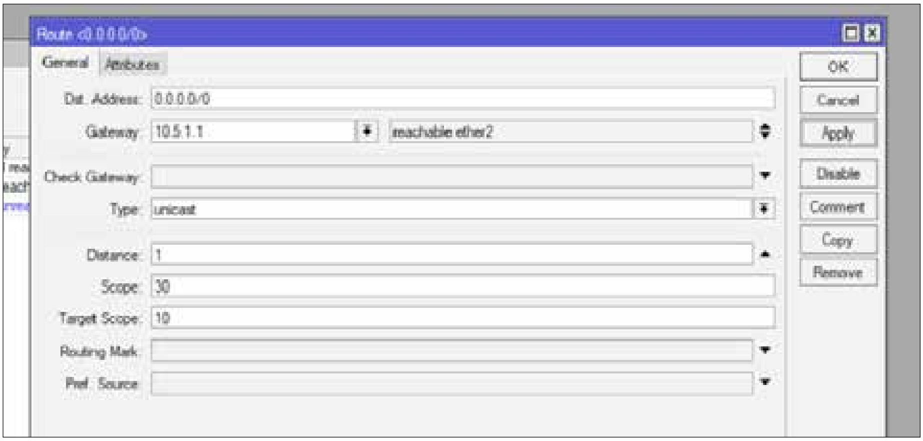
3.1 Next, we need to assign the route. Click on IP > Routes.



3.2 Click on + > assign to assign the destination address to 0.0.0.0/0 and gateway 10.5.1.1 (gateway of the input IP address).



	Dst. Address	Gateway	Distance	Routing Mark	Pref. Source
DAC	10.5.1.0/24	ether2 reachable	0		10.5.1.9
DC	10.10.10.0/24	ether6 unreachable	255		10.10.10.1



Dst. Address: 0.0.0.0/0

Gateway: 10.5.1.1 reachable ether2

Check Gateway:

Type: unicast

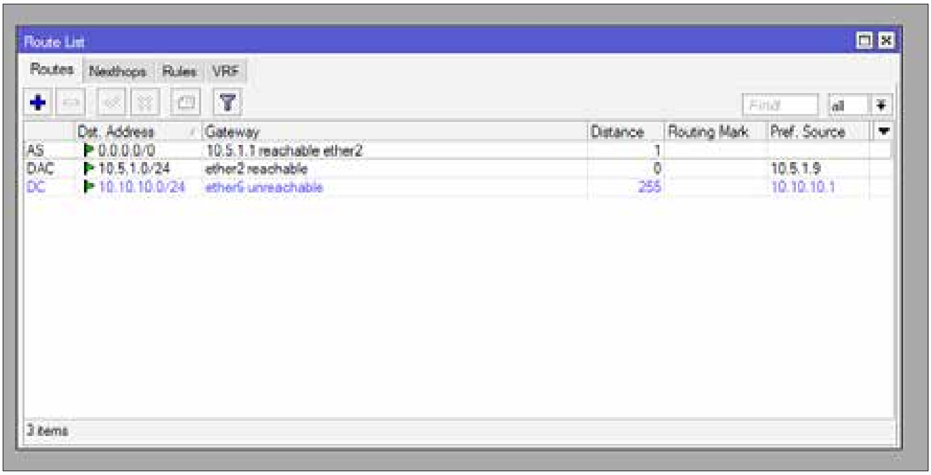
Distance: 1

Scope: 30

Target Scope: 10

Routing Mark:

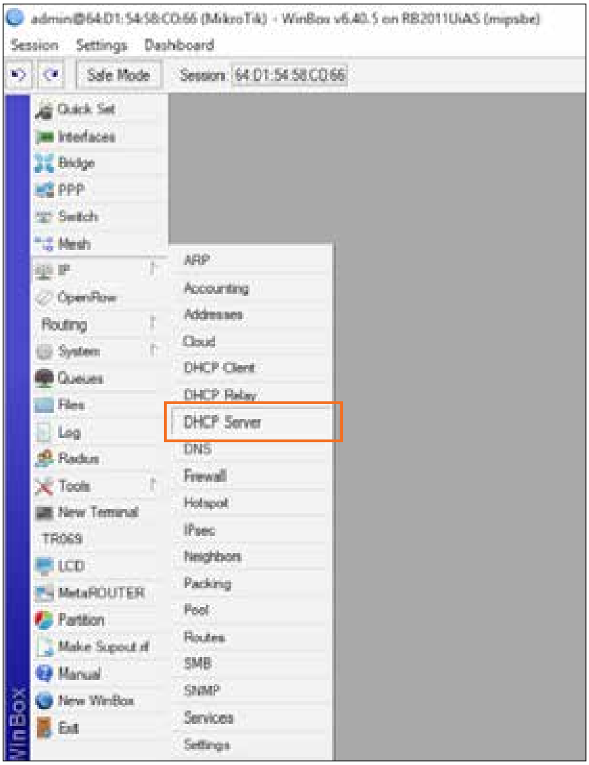
Pref. Source:



	Dst. Address	Gateway	Distance	Routing Mark	Pref. Source
AS	0.0.0.0/0	10.5.1.1 reachable ether2	1		
DAC	10.5.1.0/24	ether2 reachable	0		10.5.1.9
DC	10.10.10.0/24	ether6 unreachable	255		10.10.10.1

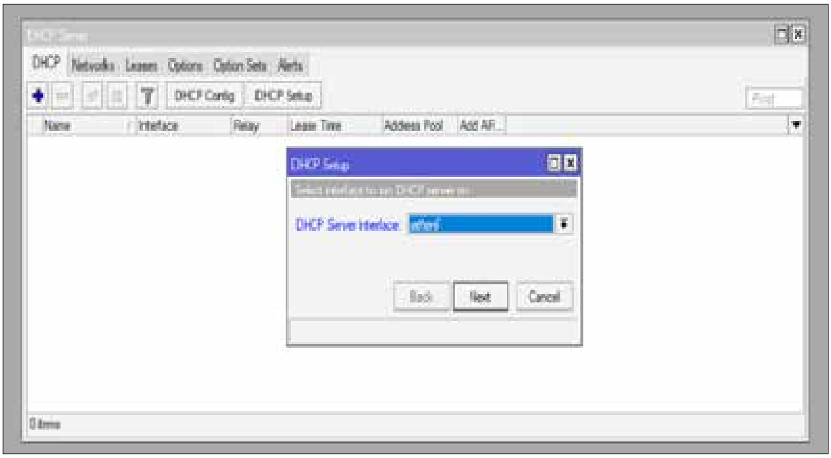
3 items

3.3 To Run DHCP on output port click on IP/ DHCP Server and click on DHCP Setup.



admin@64:D1:54:58:C0:66 (MikroTik) - WinBox v6.40.5 on RB2011UiAS (mipsbe)

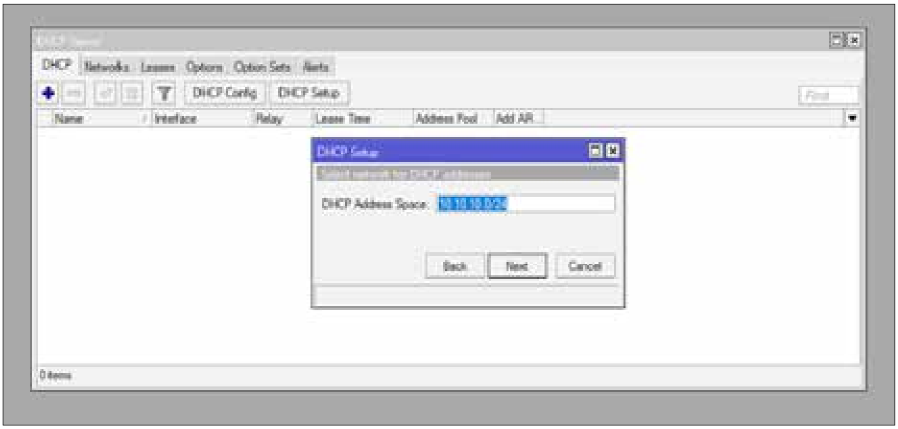
3.4 Select output interface as we are running DHCP for a local network



Select interface to run DHCP server on

DHCP Server Interface: [illegible]

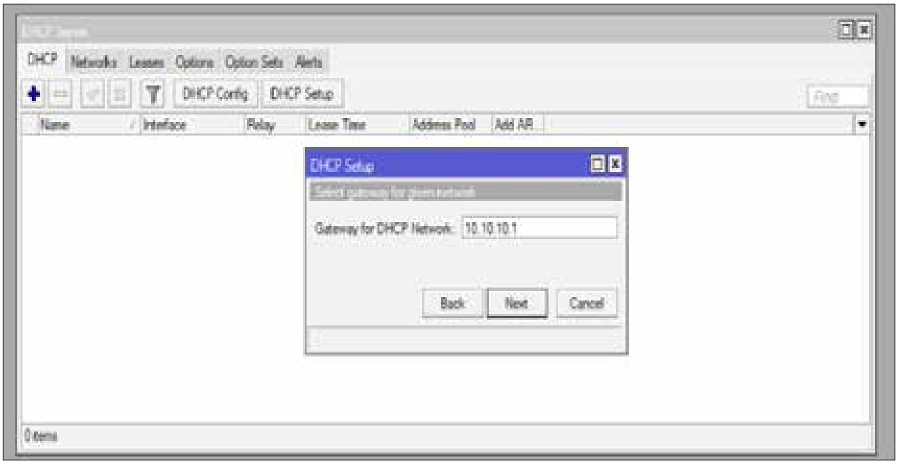
3.5 Type the output IP Address pool.



Select network for DHCP addresses

DHCP Address Space: 10.10.10.0/24

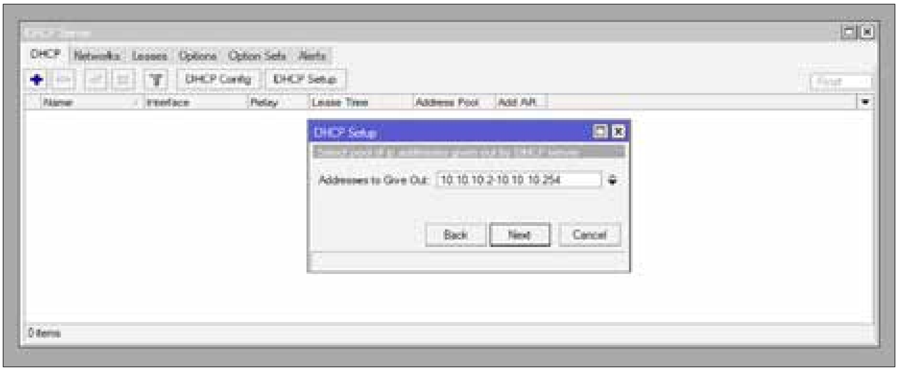
3.6 Type the gateway of the local network.



Select gateway for given network

Gateway for DHCP Network: 10.10.10.1

3.7 Type the address space we want DHCP to use

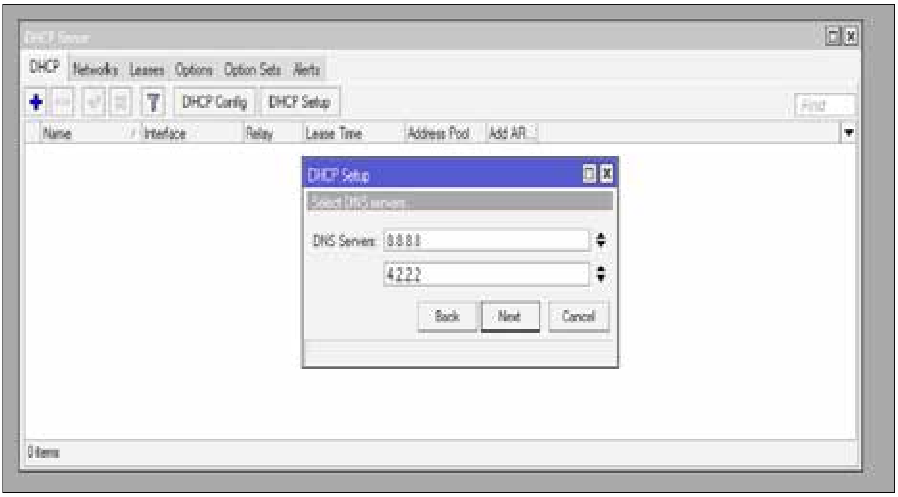


Select pool of ip addresses given out by DHCP server

Addresses to Give Out: 10.10.10.2-10.10.10.254

Setting up Wireless Networks – Part II

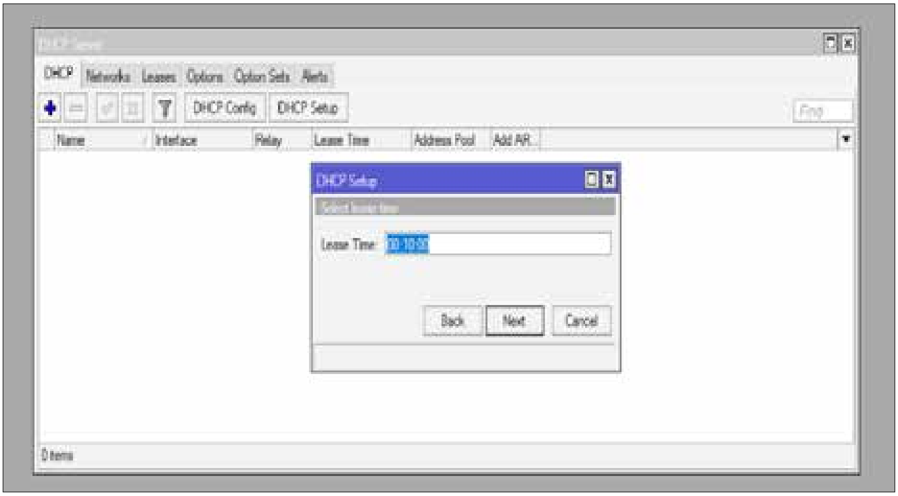
3.8 Type primary DNS and then secondary if available.



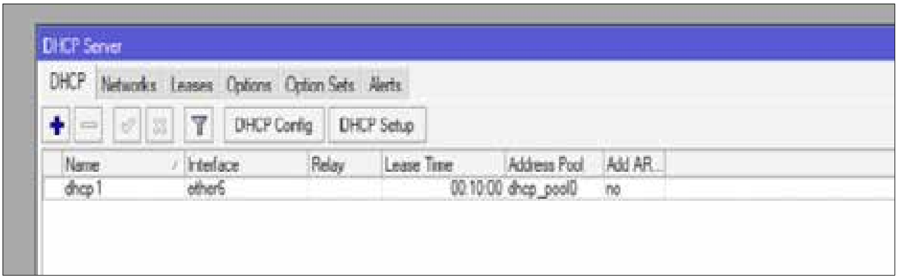
DNS Servers: 8.8.8.8

4.2.2.2

3.9 Finally, specify the lease time after which IP Address will be renewed.



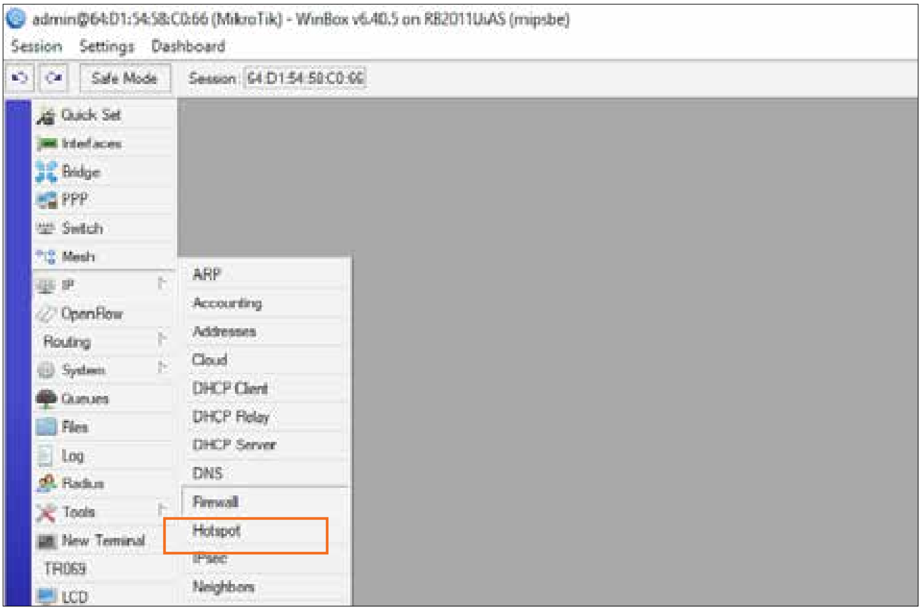
Lease Time: 00:10:00



Name	Interface	Relay	Lease Time	Address Pool	Add AR...
dhcp1	ether6		00:10:00	dhcp_pool0	no

3.10 To add firewall rules for an established connection, invalid packets and ping, click on IP and Firewall

So, you learned how to set up the router to accept connections from other devices.



To view the corresponding video on the course website, you can scan the QR Code displayed here or directly log in to the course website http://lms.defindia.org

Video Duration: 3:39 Minutes

4. Testing the device

1. Assign IP

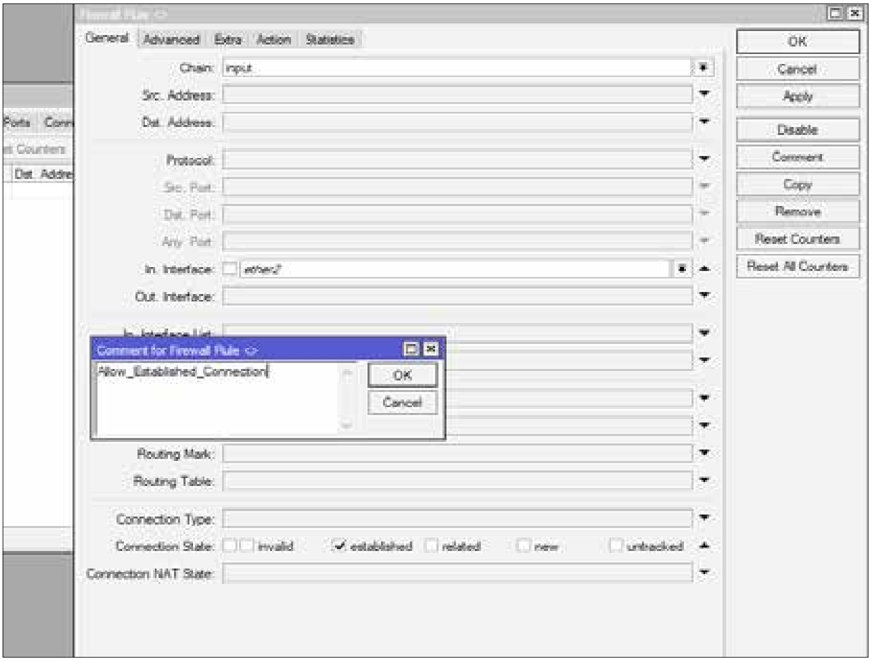
2. Secure the device

3. Create connections

4. Test the device

5. Change configuration

4.1 For accepting the packets of established connections, click on +. Select the chain to input in the interface to the input interface (ether 2), Connection state to established and for comment click on comment, finally click action to Accept.



Chain: input

Src. Address:

Dst. Address:

Protocol:

Src. Port:

Dst. Port:

Any. Port:

In. Interface: ☐ ether2

Out. Interface:

In. Interface List:

Comment for Firewall Rule <>

Allow_Established_Connection

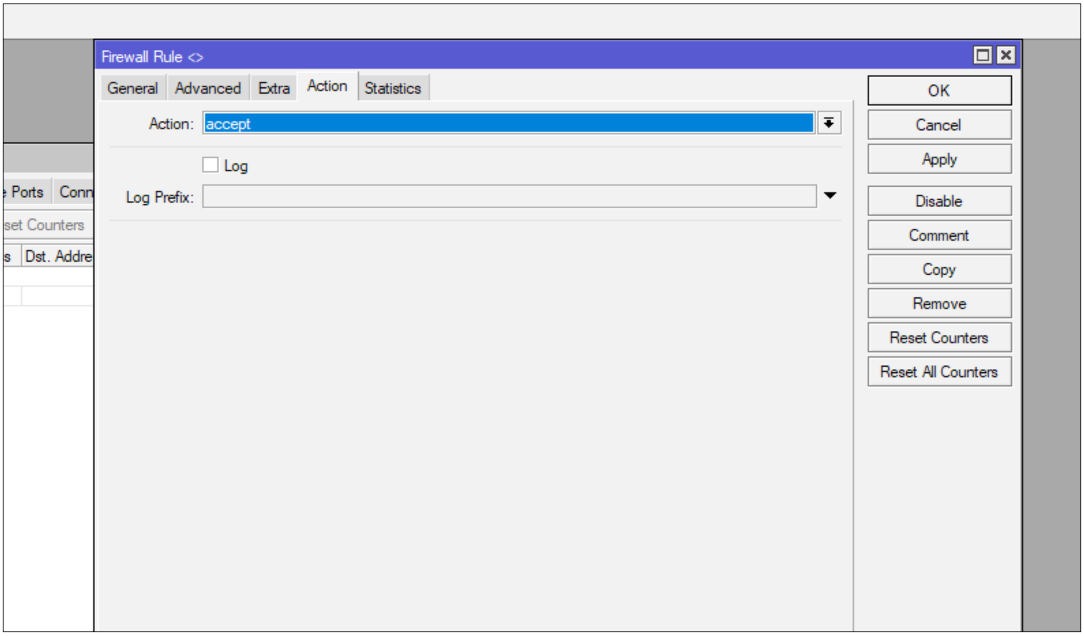
Routing Mark:

Routing Table:

Connection Type:

Connection State: ☐ ☐ invalid ☑ established ☐ related ☐ new ☐ untracked

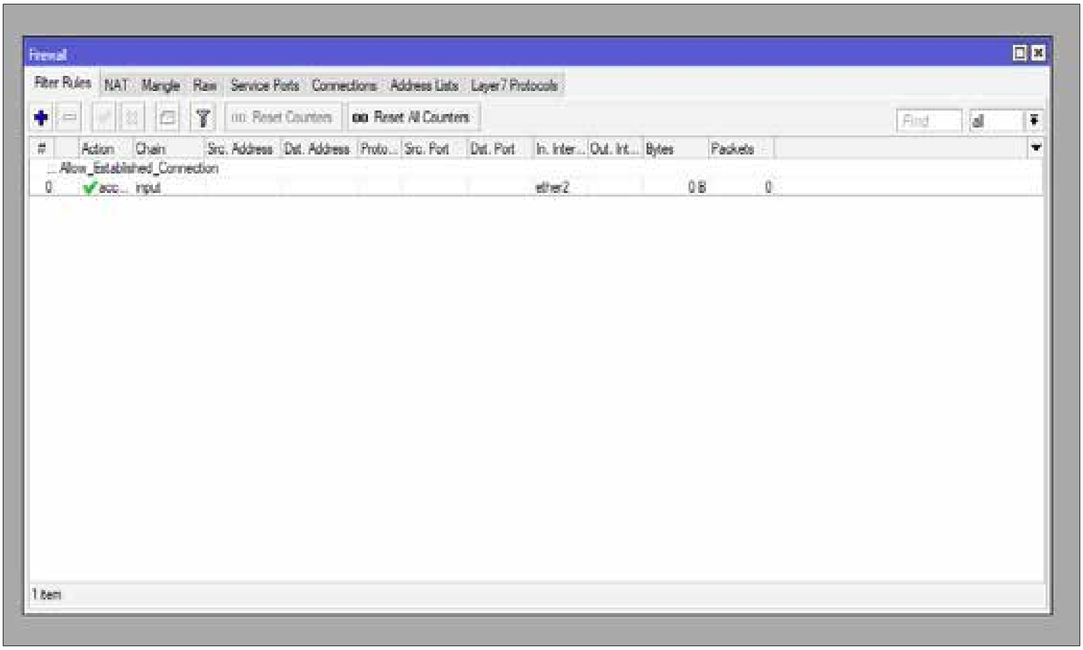
Connection NAT State:



Action: accept

□ Log

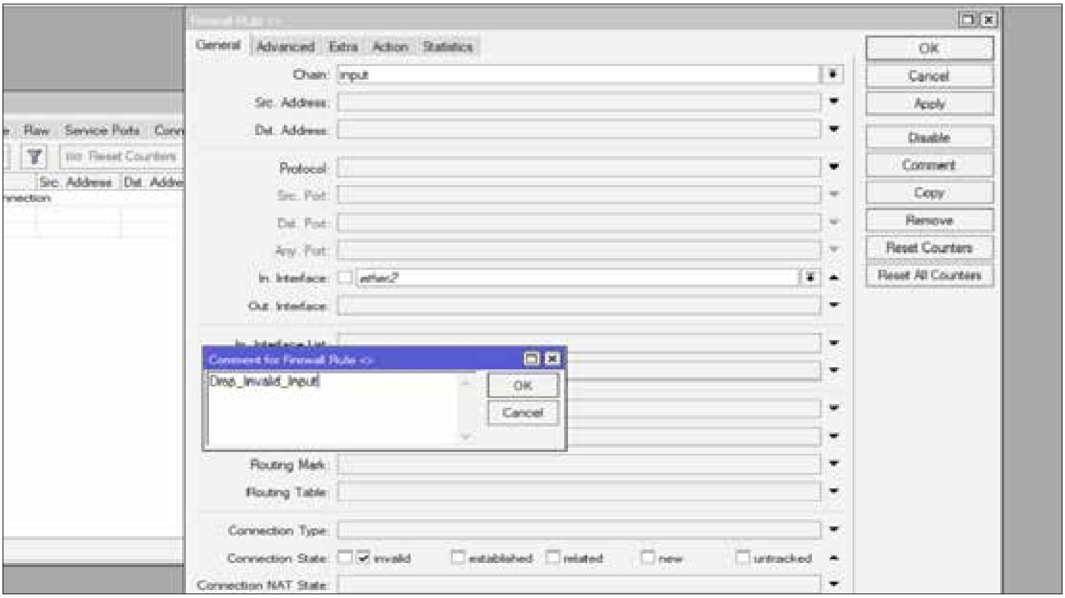
Log Prefix:



#		Action	Chain	Src. Address	Dst. Address	Proto...	Src. Port	Dst. Port	In. Inter...	Out. Int...	Bytes	Packets
;;; Allow_Established_Connection												
0		✓ acc...	input						ether2		0 B	0

1 item

4.2 To drop all the invalid packets, click on Chain to input, interface to input interface (ether2), connection state to invalid and finally action to drop.



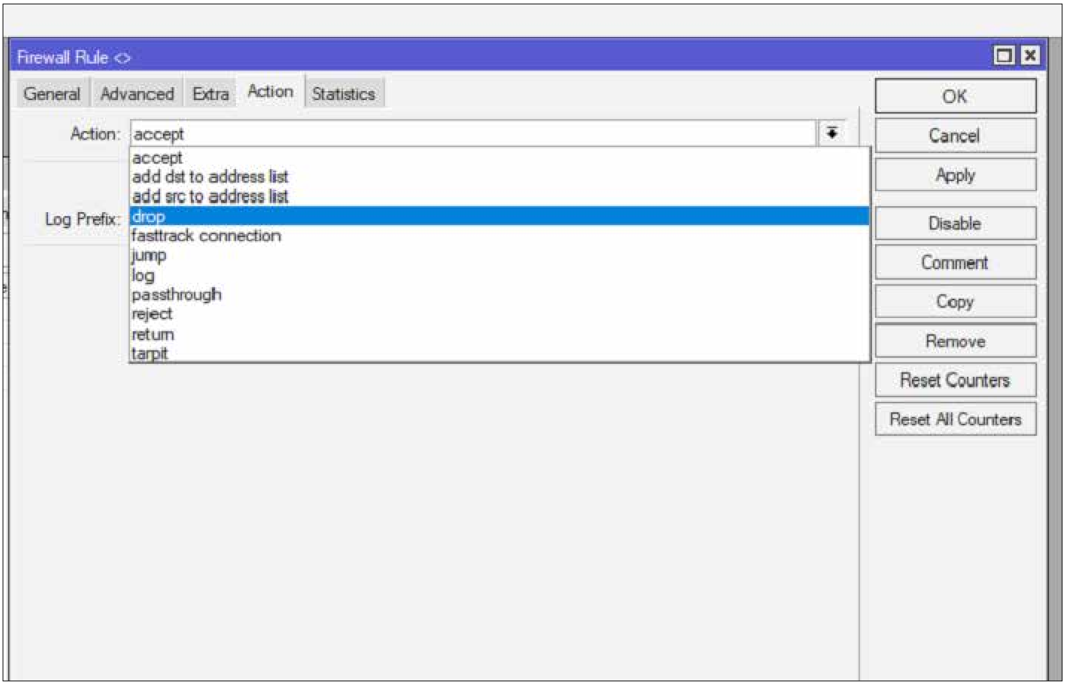
Chain: input

In. Interface: □ ether2

Connection State: □ ☑ invalid □ established □ related □ new □ untracked

Comment for Firewall Rule <>

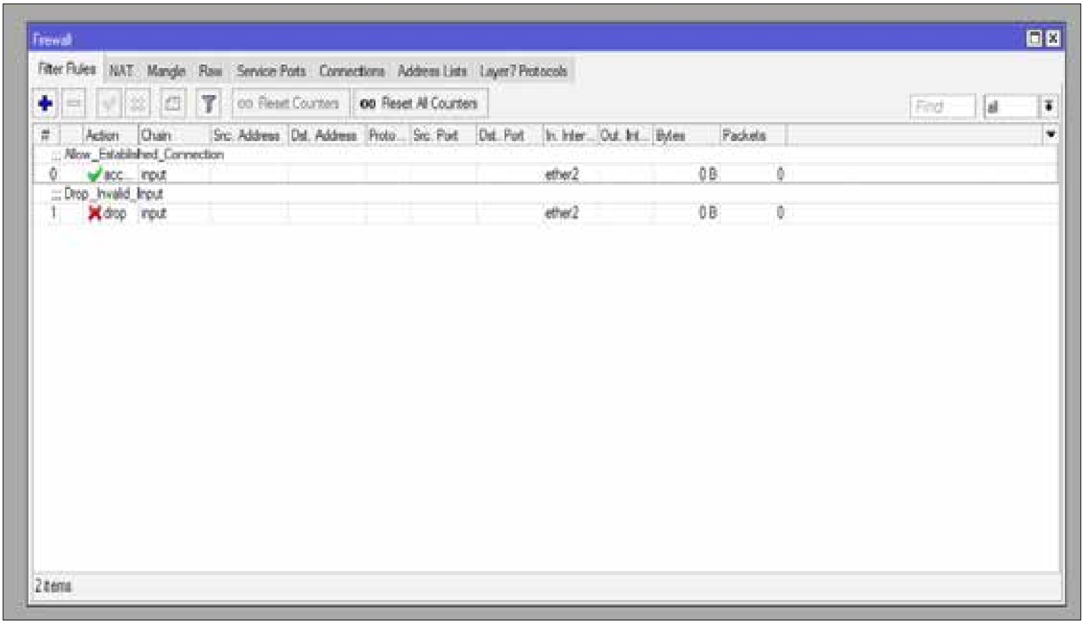
Drop_Invalid_Input



Firewall Rule <>

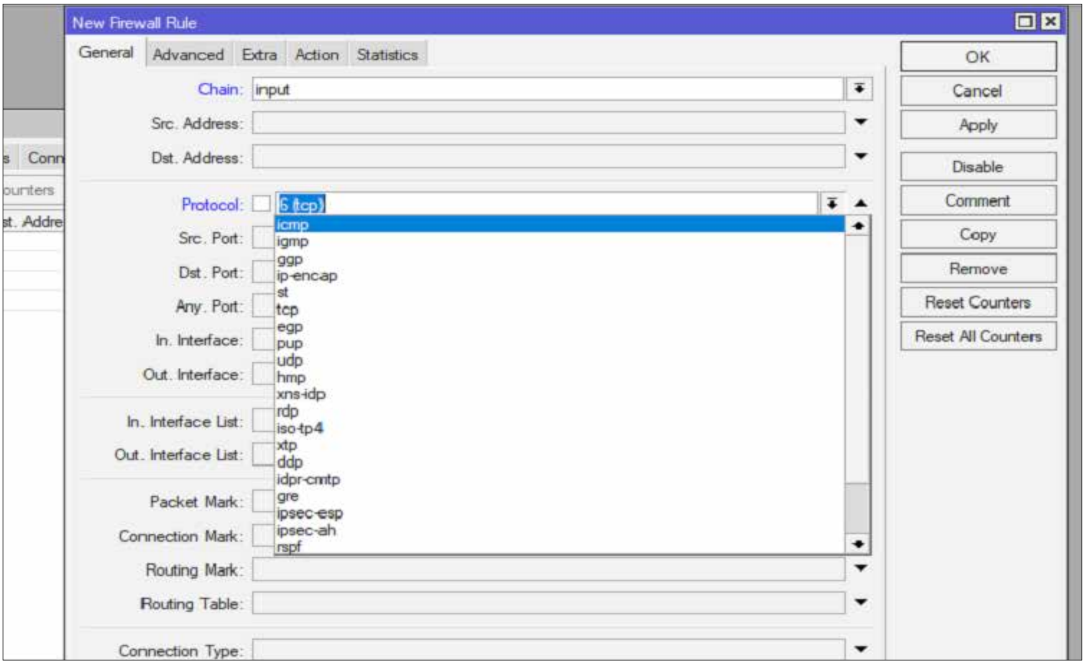
Action: accept

Log Prefix:

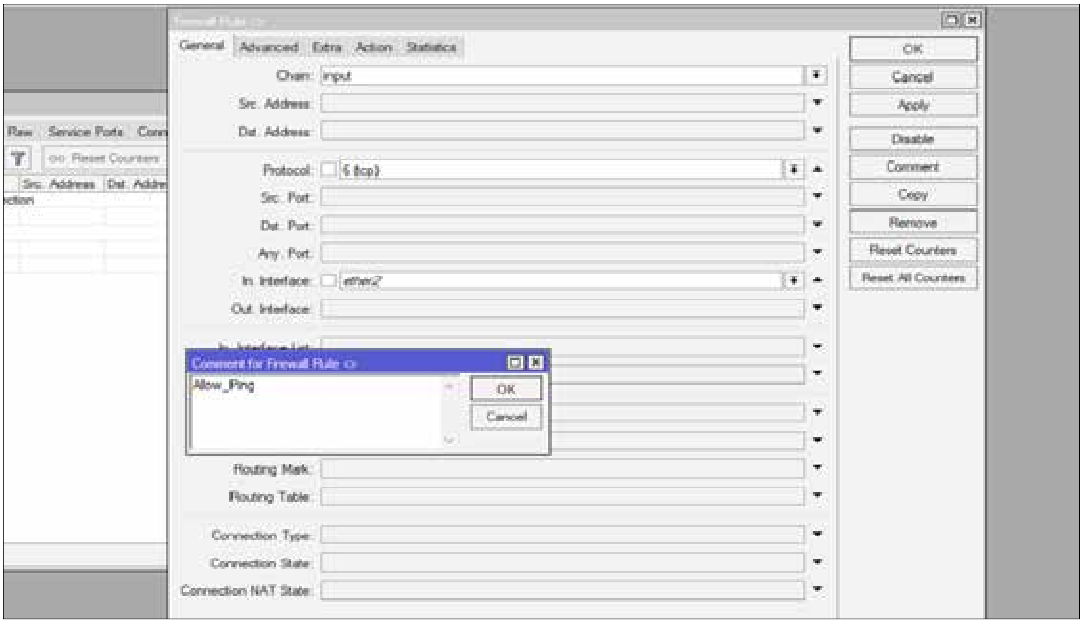


```
#   Action  Chain  Src. Address  Dst. Address  Proto...  Src. Port  Dst. Port  In. Inter...  Out. Int...  Bytes  Packets
;;; Allow_Established_Connection
0   acc...  input                                                              ether2                     0 B    0
;;; Drop_Invalid_Input
1   drop    input                                                              ether2                     0 B    0
2 items
```

4.3 To allow ping, click on chain to input, protocol to icmp, in interface to input interface (ether2) and action to accept



Chain: input
Src. Address:
Dst. Address:
Protocol: 6 (tcp)
Src. Port:
Dst. Port:
Any. Port:
In. Interface:
Out. Interface:
In. Interface List:
Out. Interface List:
Packet Mark:
Connection Mark:
Routing Mark:
Routing Table:
Connection Type:

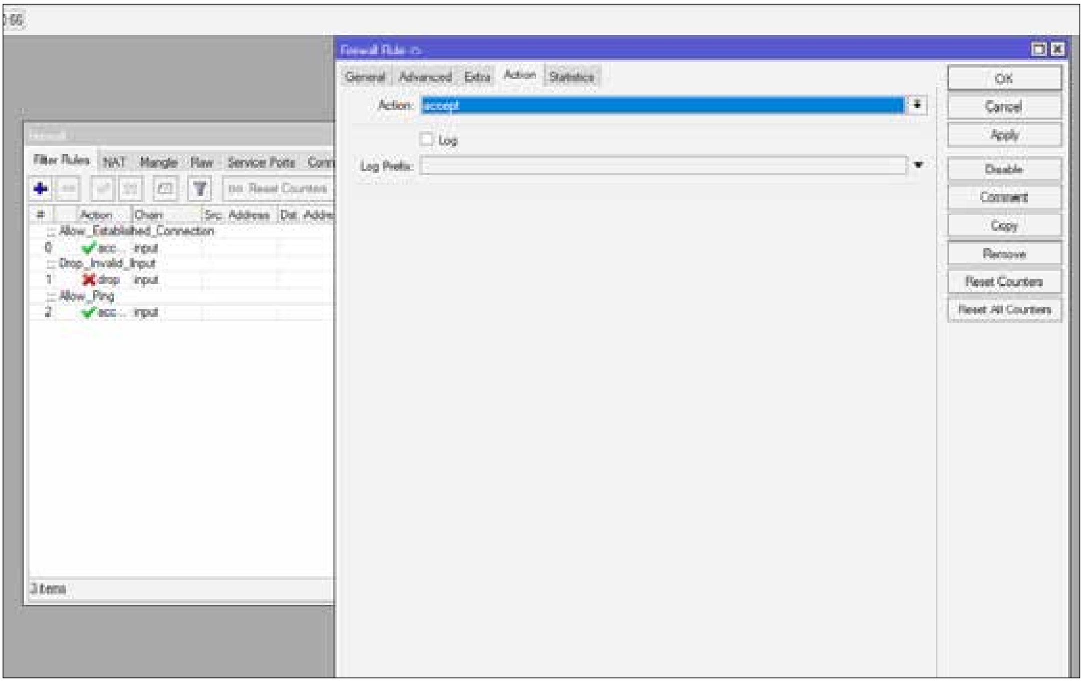


Chain: input

Protocol: 6 (tcp)

In. Interface: ether2

Comment for Firewall Rule: Allow_Ping

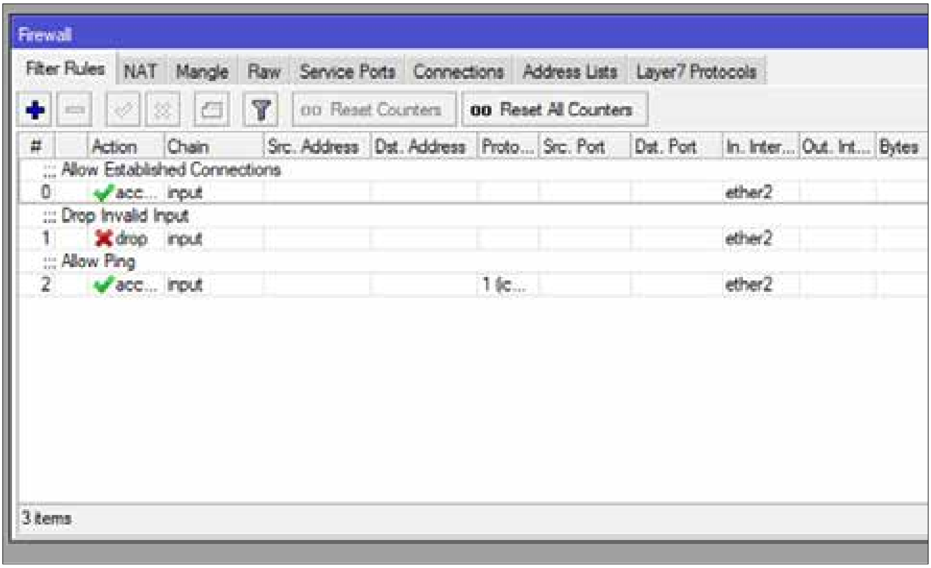


Action: accept

□ Log

Log Prefix:

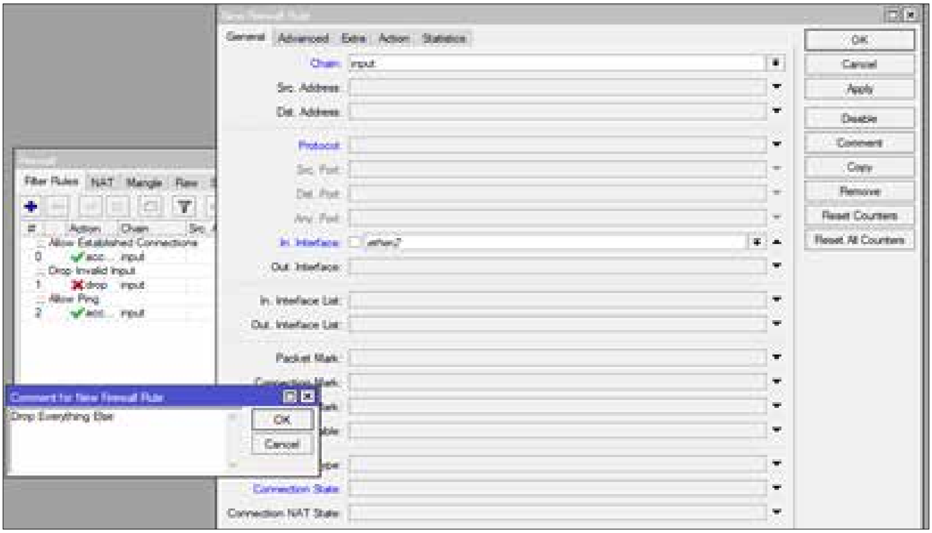
```
#   Action   Chain   Src. Address   Dst. Addre
;;; Allow_Established_Connection
0   ✓ acc... input
;;; Drop_Invalid_Input
1   ✗ drop   input
;;; Allow_Ping
2   ✓ acc... input
3 items
```



#	Action	Chain	Src. Address	Dst. Address	Proto...	Src. Port	Dst. Port	In. Inter...	Out. Int...	Bytes
::: Allow Established Connections										
0	✓acc...	input						ether2		
::: Drop Invalid Input										
1	✗drop	input						ether2		
::: Allow Ping										
2	✓acc...	input			1 (ic...			ether2		

3 items

4.4 Finally, to drop all the packets other than the entry in our firewall click on chain to input, interface to input interface (ether2) and action to drop

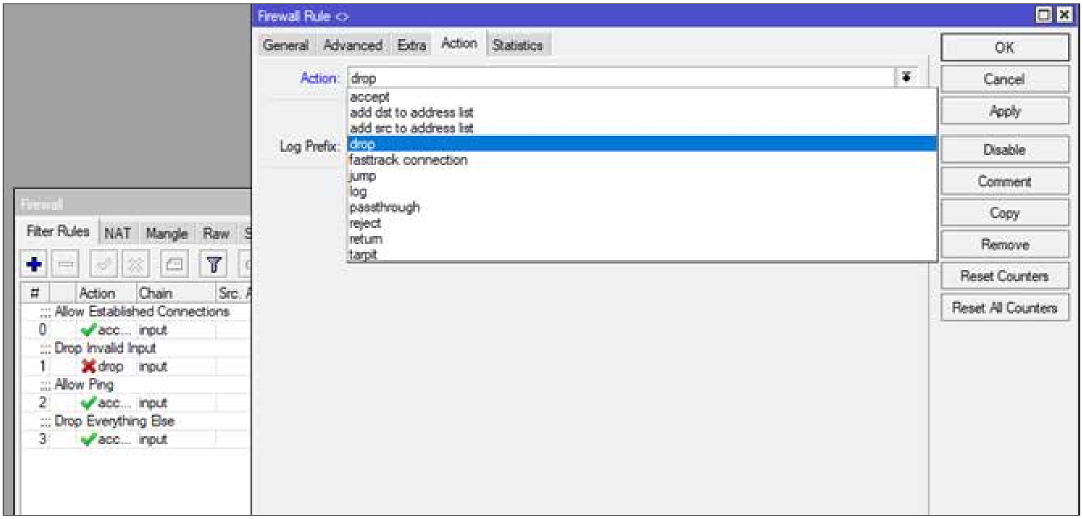


Chain: input

In. Interface: ether2

Comment for New Firewall Rule

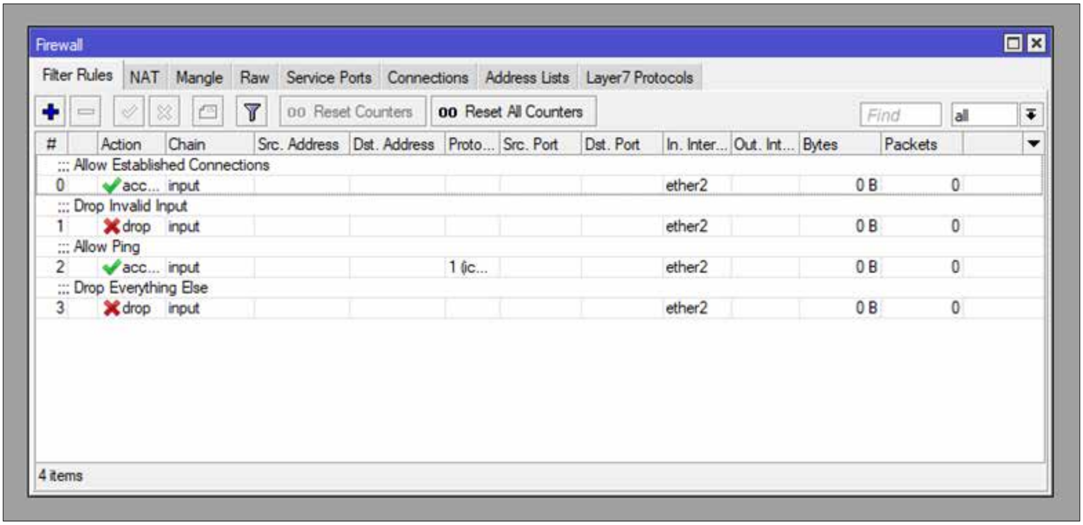
Drop Everything Else



Action: drop

Log Prefix:

#	Action	Chain	Src. A
;;; Allow Established Connections			
0	✓ acc...	input	
;;; Drop Invalid Input			
1	✗ drop	input	
;;; Allow Ping			
2	✓ acc...	input	
;;; Drop Everything Else			
3	✓ acc...	input	



#	Action	Chain	Src. Address	Dst. Address	Proto...	Src. Port	Dst. Port	In. Inter...	Out. Int...	Bytes	Packets
;;; Allow Established Connections											
0	✓ acc...	input						ether2		0 B	0
;;; Drop Invalid Input											
1	✗ drop	input						ether2		0 B	0
;;; Allow Ping											
2	✓ acc...	input			1 (ic...			ether2		0 B	0
;;; Drop Everything Else											
3	✗ drop	input						ether2		0 B	0

4 items

You learned about the steps to test if the router is working. You have now learned about all the steps involved in configuring the router.

5. Changing the configuration

1. Assign IP

2. Secure the device

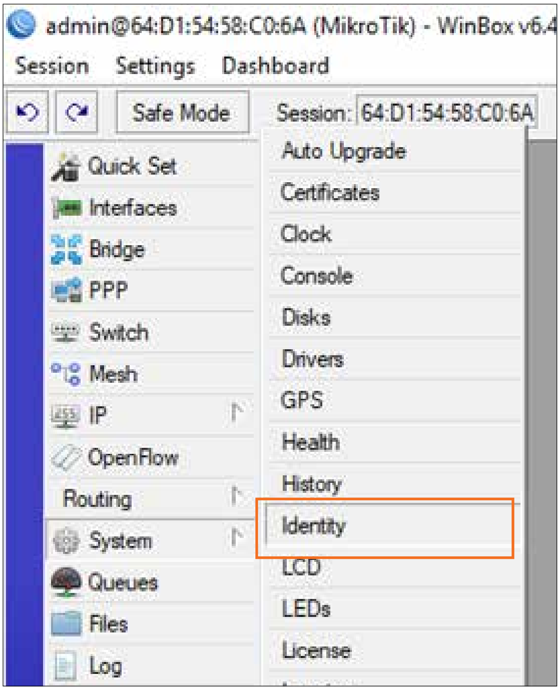
3. Create connections

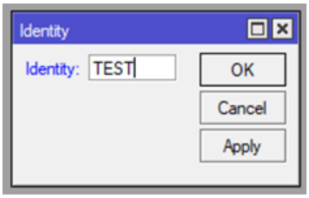
4. Test the device

5. Change configuration

Once you start using the network, you might want to change the configuration. Let us look at the steps for changing some of the configuration parameters.

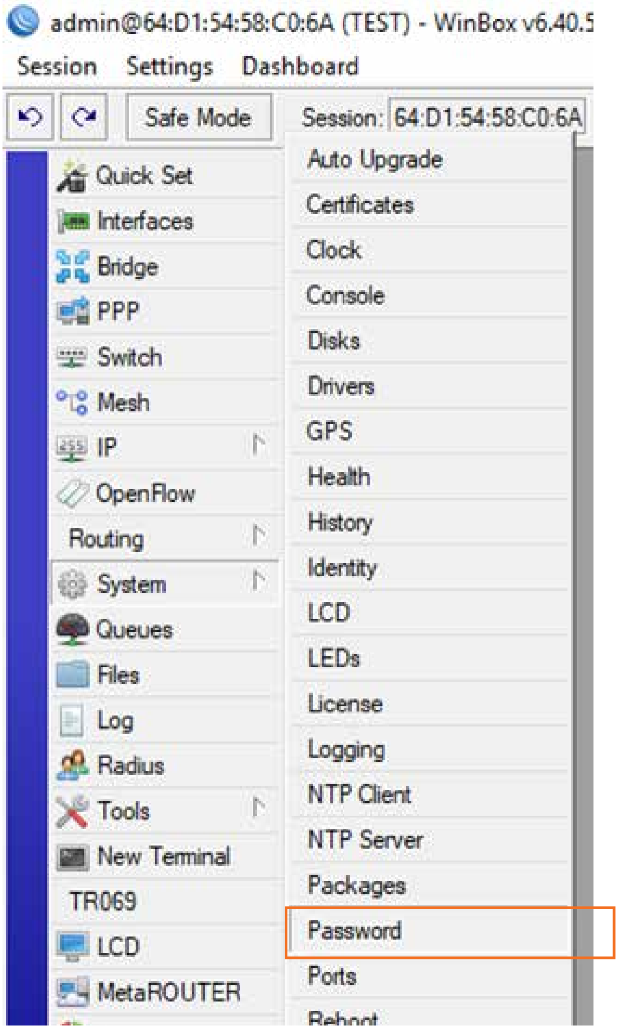
5.1 To Change the name of the router, click on system and identity

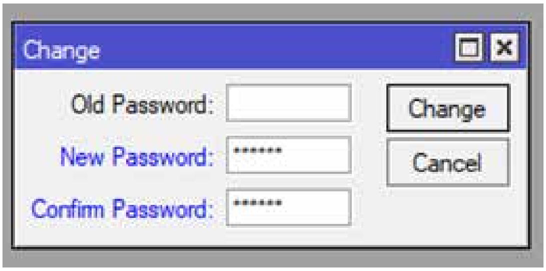




Identity: TEST

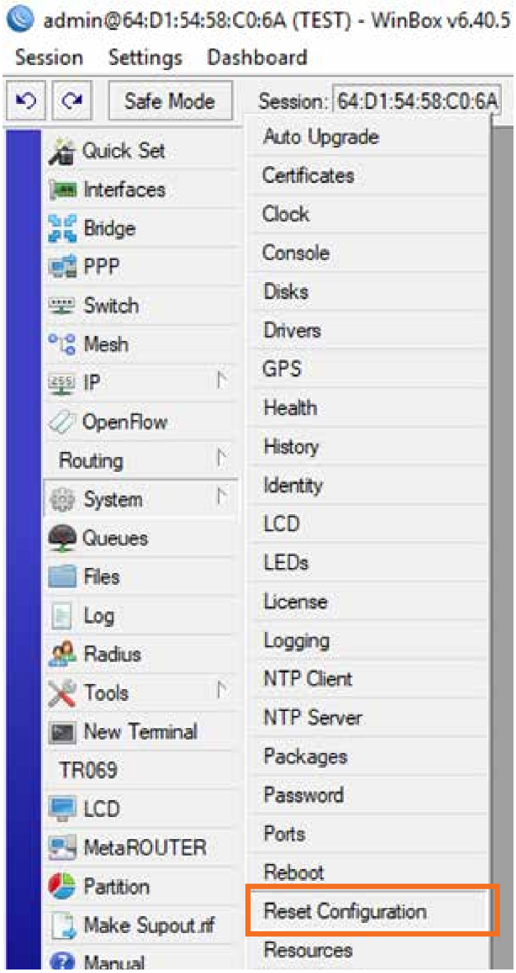
5.2 To change the password of the router, click on system/ password. Type the old password if available and then the new password and confirm the password.

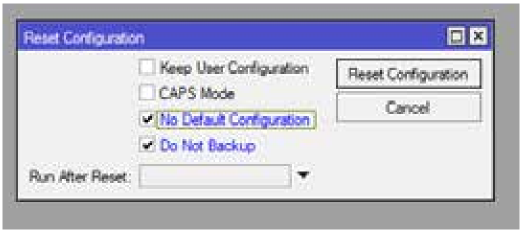




Old Password:
New Password: *******
Confirm Password: *******

5.3 To reset the router, click on system/ reset configuration and check on No default configuration and Do Not Backup and then click on reset configuration.





□ Keep User Configuration
□ CAPS Mode
☑ No Default Configuration
☑ Do Not Backup
Run After Reset:

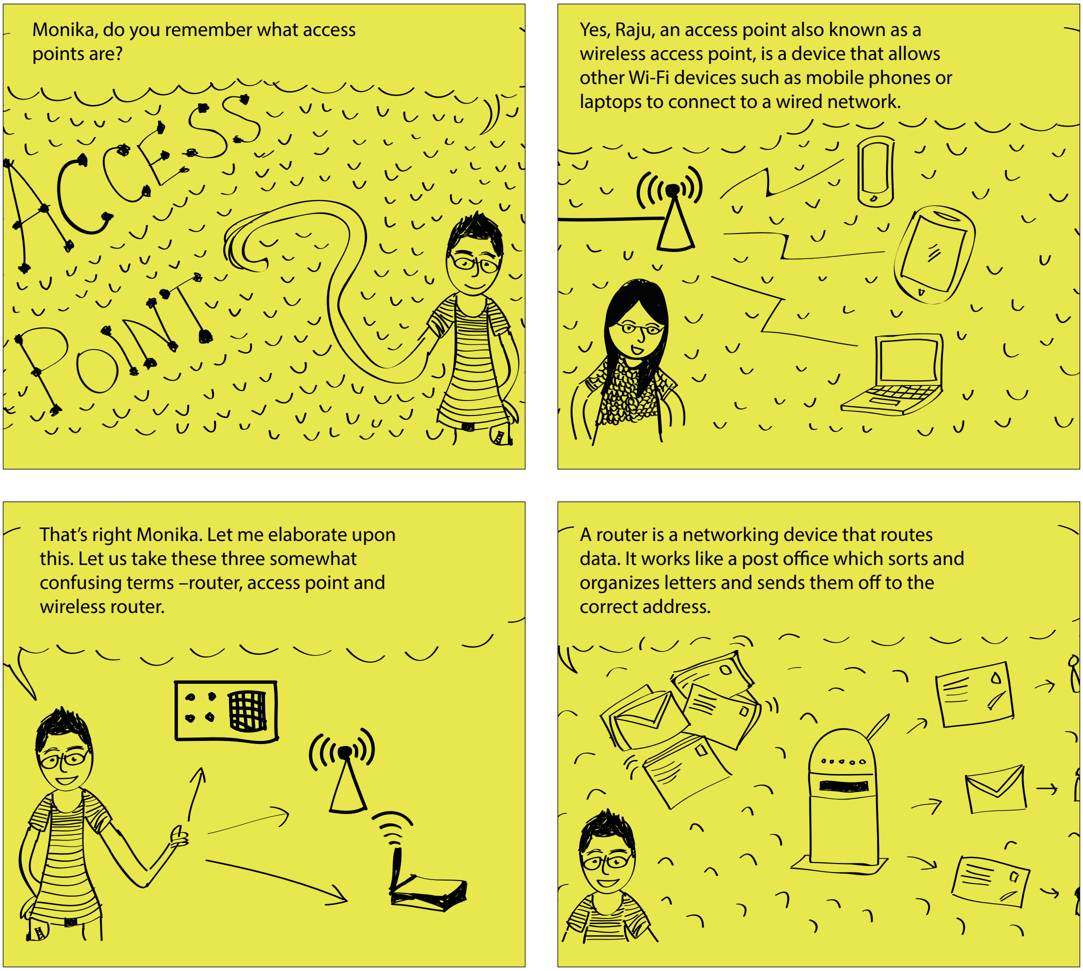
!

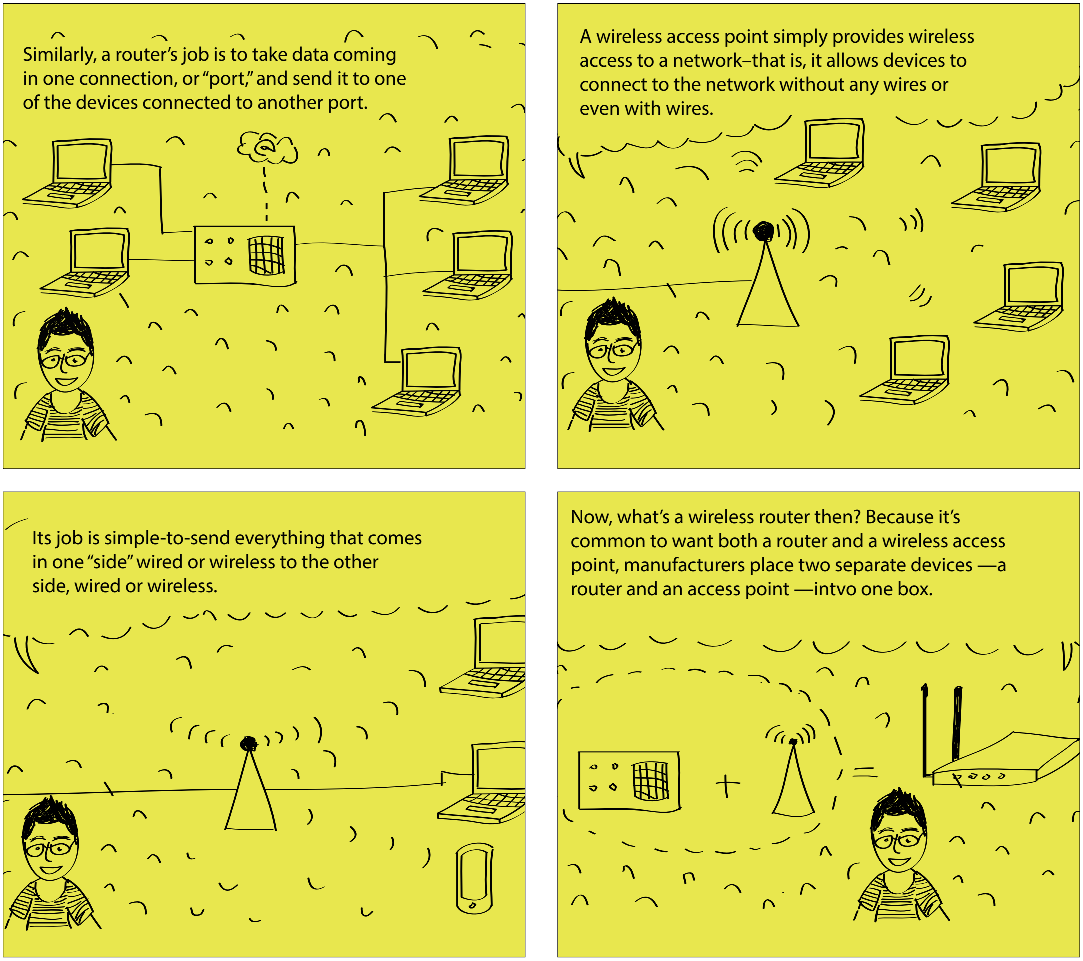
To view the corresponding video on the course website, you can scan the QR Code displayed here or directly log in to the course website http://lms.defindia.org

Video Duration: 3:32 Minutes

Configuring Access Points

Now that the router is configured, we need to configure the wireless access points. This will enable customers who have subscribed to your Internet services to use the internet on their devices.


Monika, do you remember what access points are?
ACCESS POINT
Yes, Raju, an access point also known as a wireless access point, is a device that allows other Wi-Fi devices such as mobile phones or laptops to connect to a wired network.
That's right Monika. Let me elaborate upon this. Let us take these three somewhat confusing terms –router, access point and wireless router.
A router is a networking device that routes data. It works like a post office which sorts and organizes letters and sends them off to the correct address.


Similarly, a router's job is to take data coming in one connection, or "port," and send it to one of the devices connected to another port.
A wireless access point simply provides wireless access to a network–that is, it allows devices to connect to the network without any wires or even with wires.
Its job is simple-to-send everything that comes in one "side" wired or wireless to the other side, wired or wireless.
Now, what's a wireless router then? Because it's common to want both a router and a wireless access point, manufacturers place two separate devices —a router and an access point —intvo one box.
+
=

!

To view the corresponding video on the course website, you can scan the QR Code displayed here or directly log in to the course website http://lms.defindia.org

Video Duration: 1:50 Minutes

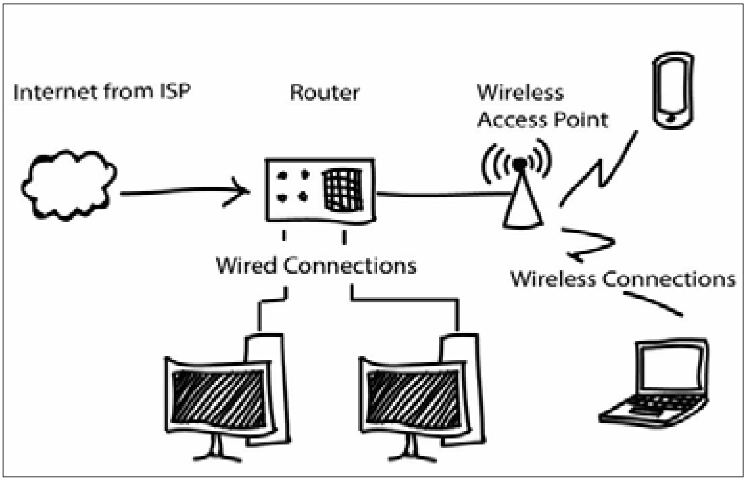


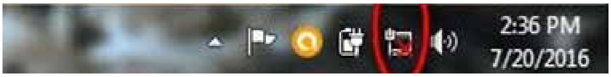
Figure 8: Role of the router and wireless access Point

For the purpose of this section, we will assume you have a Ubiquity Radio access point.

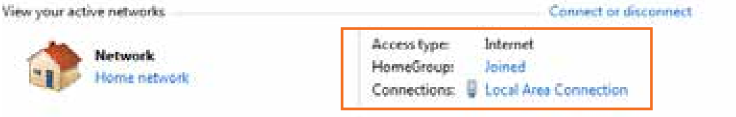
Assigning an IP address to a laptop to access the Ubiquity Radio

Before we actually configure the ubiquity radio, we need to assign an IP address to the laptop that will be used to access the ubiquity radio.

1. First, locate the icon for the local area connection. This is usually on the taskbar on a Windows laptop. Click on the icon.



A window will be displayed.



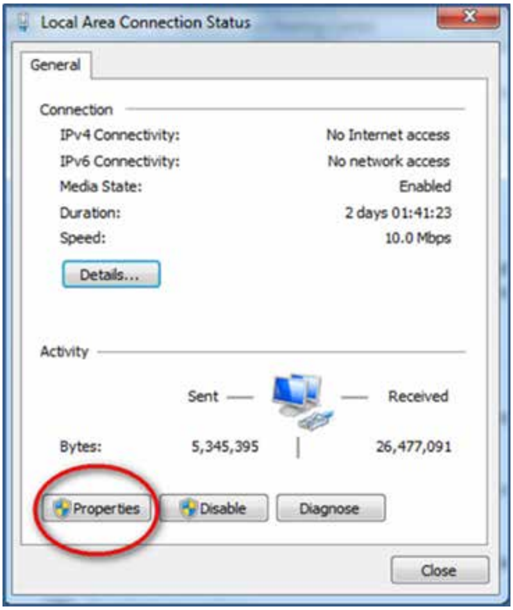
View your active networks

Connect or disconnect

Network
Home network

Access type: Internet
HomeGroup: Joined
Connections: Local Area Connection

2. Click on Properties. Another window will be displayed.



Connection

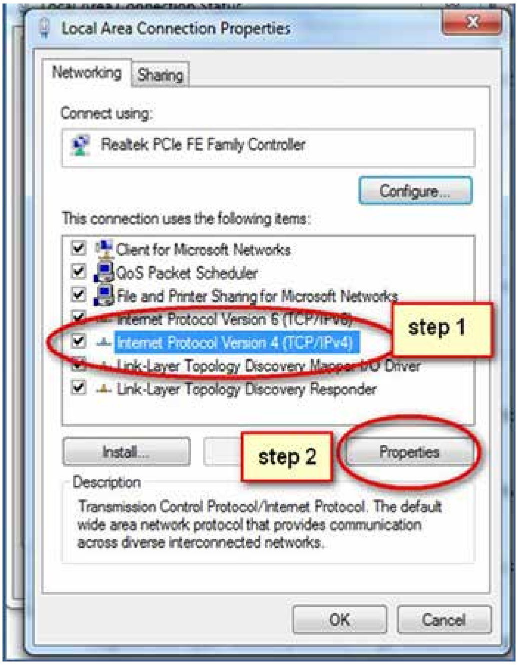
IPv4 Connectivity: No Internet access
IPv6 Connectivity: No network access
Media State: Enabled
Duration: 2 days 01:41:23
Speed: 10.0 Mbps

Activity

Sent — Received

Bytes: 5,345,395 | 26,477,091

3. Click on Internet Protocol Version 4 (TCP/IPv4) and then double-click on Properties.



Connect using:

Realtek PCIe FE Family Controller

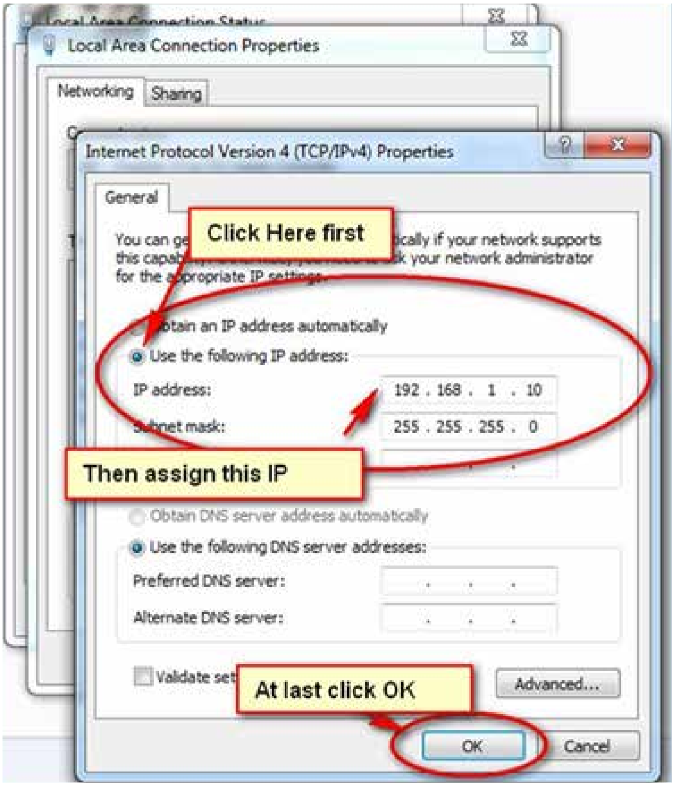
This connection uses the following items:

☑ Client for Microsoft Networks
☑ QoS Packet Scheduler
☑ File and Printer Sharing for Microsoft Networks
☑ Internet Protocol Version 6 (TCP/IPv6)
☑ Internet Protocol Version 4 (TCP/IPv4)
☑ Link-Layer Topology Discovery Mapper I/O Driver
☑ Link-Layer Topology Discovery Responder

Description

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

4. Assign this IP address to access the radio. After clicking OK, close every open window.



Internet Protocol Version 4 (TCP/IPv4) Properties

General

You can ge... ...ically if your network supports this capab... ...k your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 192 . 168 . 1 . 10

Subnet mask: 255 . 255 . 255 . 0

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .

□ Validate set...

Advanced...

OK

Cancel

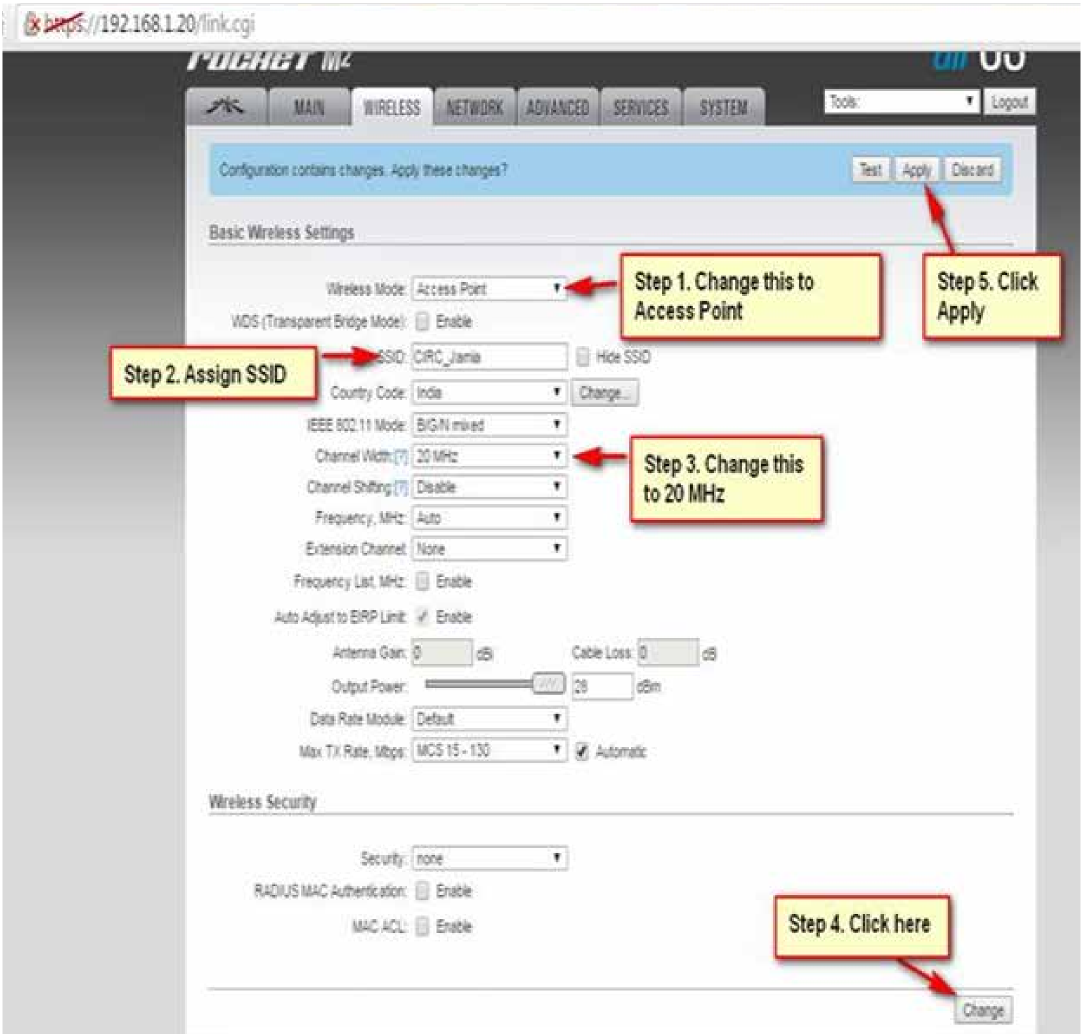
!

To view the corresponding video on the course website, you can scan the QR Code displayed here or directly log in to the course website http://lms.defindia.org

Video Duration: 0:58 Seconds

Configuring the Ubiquity Radio

1. Open any web browser on the laptop configured. Type 192.168.1.20 in the address bar. The following screen will be displayed.
2. Provide all the required details. Username and Passwords are "ubnt". Change the Country to India and Language to English. Check the shown option and at last click on Login.
3. On the page below, we need to configure Wireless Settings. Follow the image which shows step by step configuration.



~~https~~://192.168.1.20/link.cgi

Configuration contains changes. Apply these changes?

Basic Wireless Settings

Wireless Mode: Access Point

WDS (Transparent Bridge Mode): □ Enable

SSID: CIRC_Jamia □ Hide SSID

Country Code: India

IEEE 802.11 Mode: B/G/N mixed

Channel Width:[?] 20 MHz

Channel Shifting:[?] Disable

Frequency, MHz: Auto

Extension Channel: None

Frequency List, MHz: □ Enable

Auto Adjust to EIRP Limit: ☑ Enable

Antenna Gain: 0 dBi Cable Loss: 0 dB

Output Power: 28 dBm

Data Rate Module: Default

Max TX Rate, Mbps: MCS 15 - 130 ☑ Automatic

Wireless Security

Security: none

RADIUS MAC Authentication: □ Enable

MAC ACL: □ Enable

Step 1. Change this to Access Point

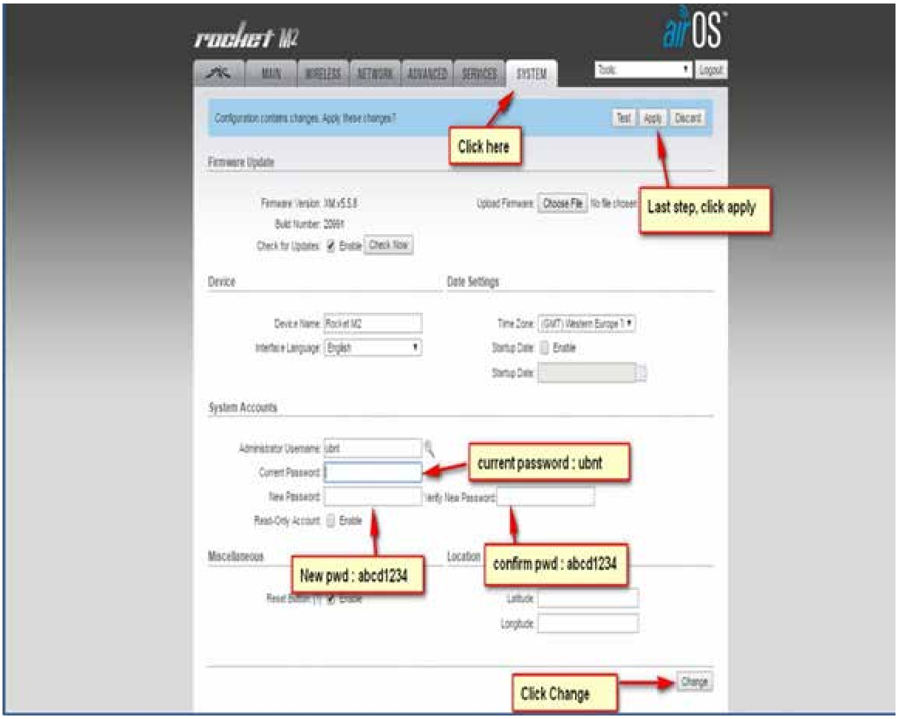
Step 2. Assign SSID

Step 3. Change this to 20 MHz

Step 4. Click here

Step 5. Click Apply

4. After configuring the wireless interface, we need to change the password to login to the device to make it secure. Please see the image below.



Configuration contains changes. Apply these changes?

Click here

Last step, click apply

Firmware Update

Firmware Version: XM.v5.5.8

Build Number: 20691

Check for Updates: ☑ Enable

Upload Firmware: No file chosen

Device

Device Name: Rocket M2

Interface Language: English

Date Settings

Time Zone: (GMT) Western Europe 1

Startup Date: □ Enable

Startup Date:

System Accounts

Administrator Username: ubnt

Current Password:

New Password:

Verify New Password:

Read-Only Account: □ Enable

current password : ubnt

New pwd : abcd1234

confirm pwd : abcd1234

Miscellaneous

Reset Button: [?] ☑ Enable

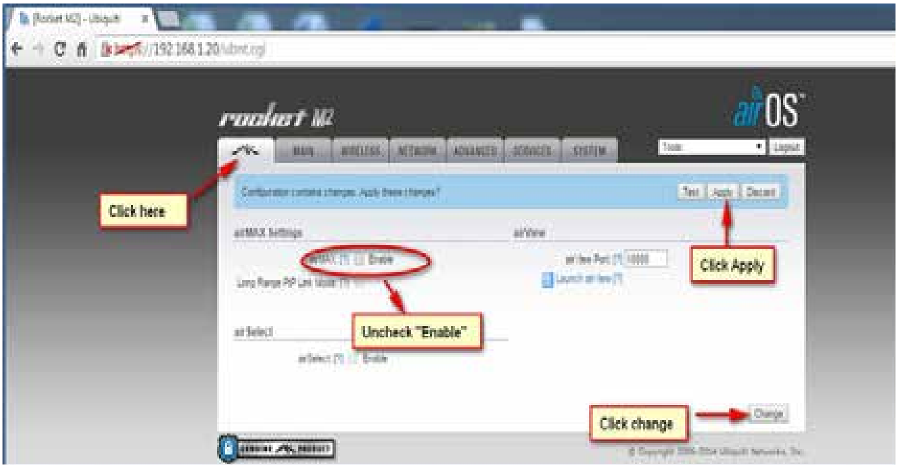
Location

Latitude:

Longitude:

Click Change

5. There is one final step we need to follow in order to finally configure our Access Point. On the First Tab of the page, we need to uncheck "Enable airMax" in order to let every other device to connect to our AP.



https://192.168.1.20/ubnt.cgi

Click here

Configuration contains changes. Apply these changes?

airMAX Settings

airMAX: [?] □ Enable

Long Range PtP Link Mode: [?]

airView

airView Port: [?] 18888

Launch airView [?]

Click Apply

Uncheck "Enable"

airSelect

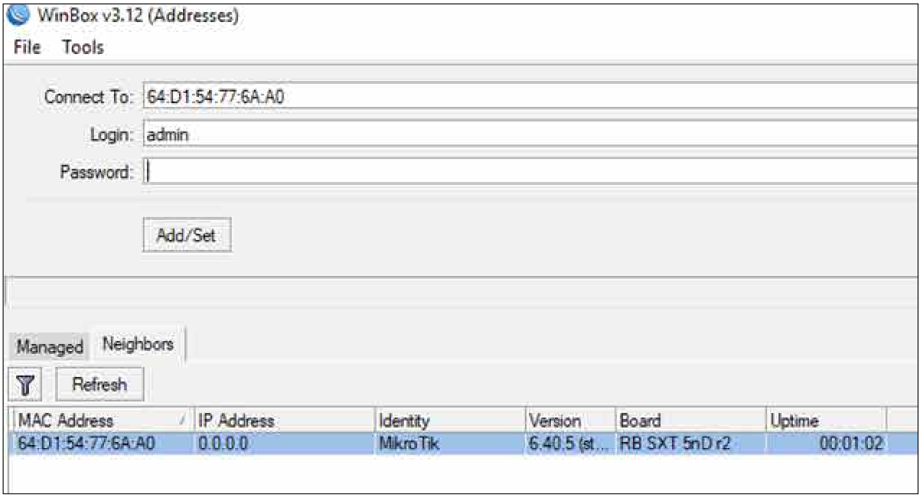
airSelect: [?] □ Enable

Click change

© Copyright 2006-2014 Ubiquiti Networks, Inc.

Configuring Mikrotik Devices

The next step is to configure the broadcasting devices from the location we need to broadcast or provide the internet. We use Omnitik and SXT to broadcast. Both devices are manufactured by Mikrotik. To access a Mikrotik Device, we need a software called "Winbox" which is also compiled by Mikrotik itself. Since SXT and Omnitik both are Mikrotik devices, we have a similar interface for both the devices and shall be having the same tutorial for them. Please follow the below pictures to have a better understanding of the same.



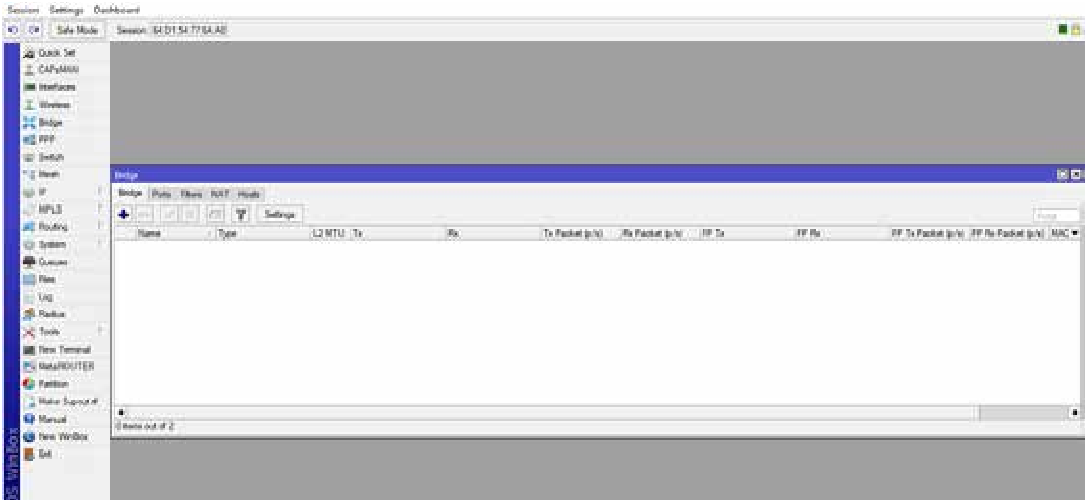
Connect To: 64:D1:54:77:6A:A0

Login: admin

Password:

MAC Address	IP Address	Identity	Version	Board	Uptime
64:D1:54:77:6A:A0	0.0.0.0	MikroTik	6.40.5 (st...	RB SXT 5nD r2	00:01:02

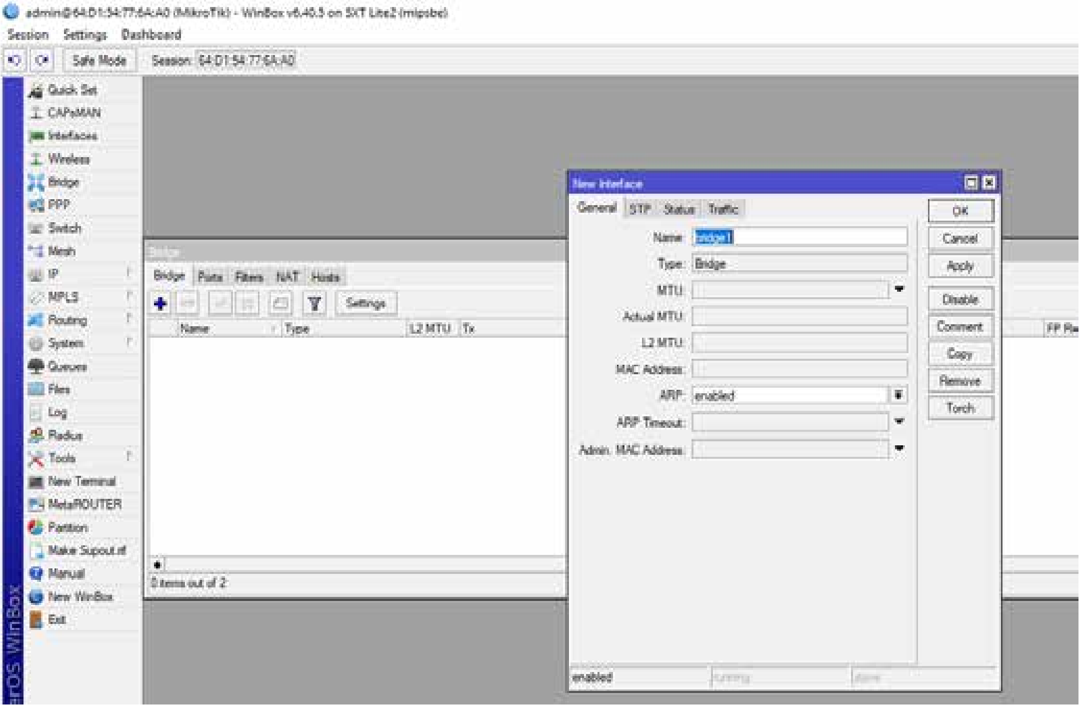
1. Connect your laptop/PC to the device directly using a straight through LAN cable. After establishing a connection, follow the above instructions. The default username is "admin" and the default password is left blank as seen above.
2. After login into the device, we need to add virtual bridge interface so as to make communication between wireless and Ethernet interfaces easily possible. Follow the above instructions for the same.



Session: 64:D1:54:77:6A:A0

0 items out of 2

3. After opening the bridge window, click on + to add a new bridge and type down its name, as shown above.



admin@64:D1:54:77:6A:A0 (MikroTik) - WinBox v6.40.5 on SXT Lite2 (mipsbe)

Session: 64:D1:54:77:6A:A0

0 items out of 2

Name: bridge1

Type: Bridge

MTU:

Actual MTU:

L2 MTU:

MAC Address:

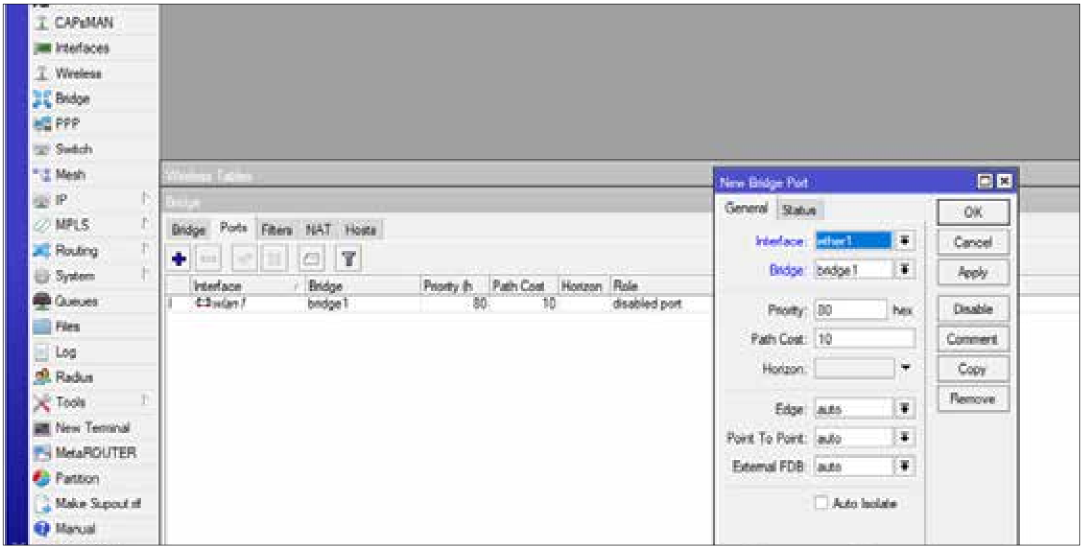
ARP: enabled

ARP Timeout:

Admin. MAC Address:

enabled

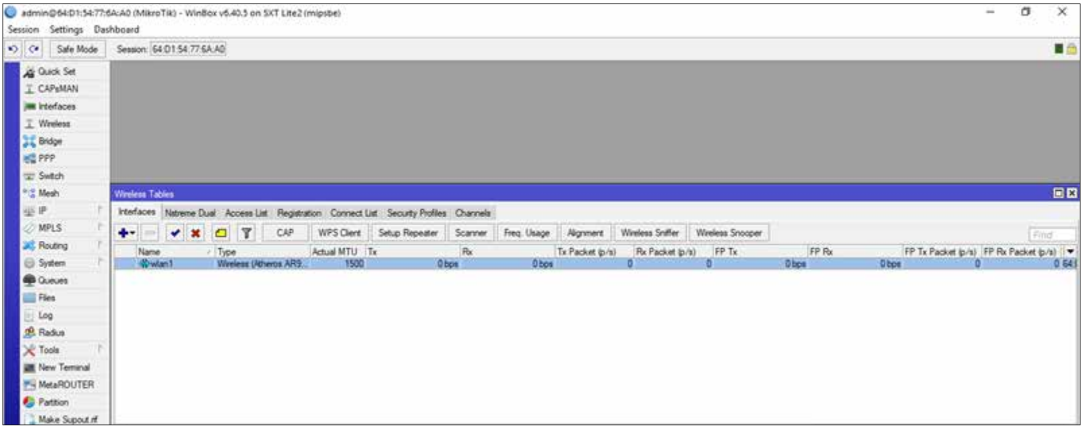
4. In the above picture, you can see the currently added bridge. Next, we need to add ports to it, through which we need our data to flow. Follow the below picture for the same.
5. In the above picture, we have added the WLAN interface. Repeat this steps until all available interfaces are added to the same bridge, namely Ether1, Ether2, Ether3, Ether4 and Ether5 along with WLAN1. Click OK to finalise.



Interface	Bridge	Priority (h	Path Cost	Horizon	Role
wlan1	bridge1	80	10		disabled port

Interface: ether1
Bridge: bridge1
Priority: 80 hex
Path Cost: 10
Horizon:
Edge: auto
Point To Point: auto
External FDB: auto
☐ Auto Isolate

6. After adding the bridge and interfaces, we need to assign an IP address to the bridge. This address will be the management IP for our device; it will be very useful in our running network. Follow the above picture to add the IP address.

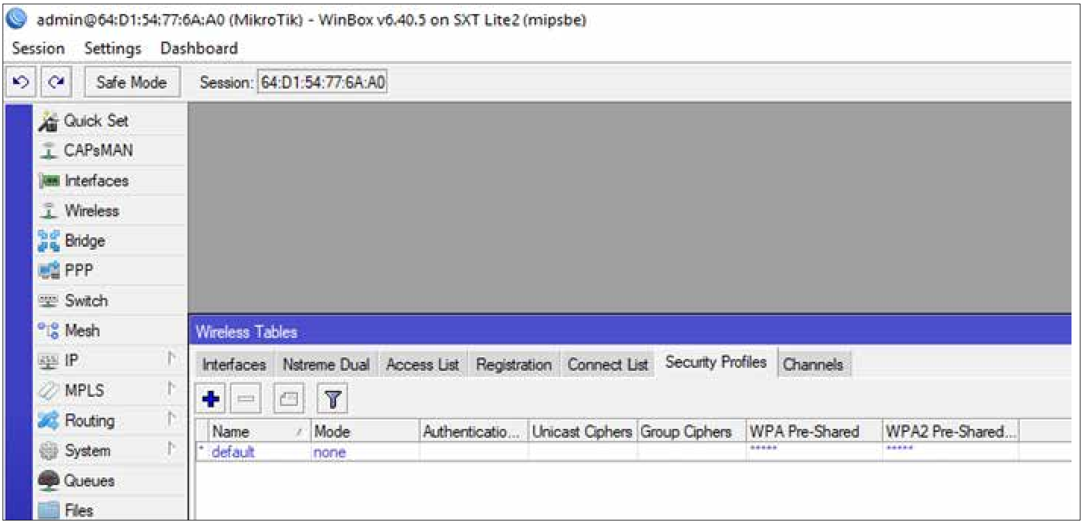


admin@64:D1:54:77:6A:A0 (MikroTik) - WinBox v6.40.5 on SXT Lite2 (mipsbe)

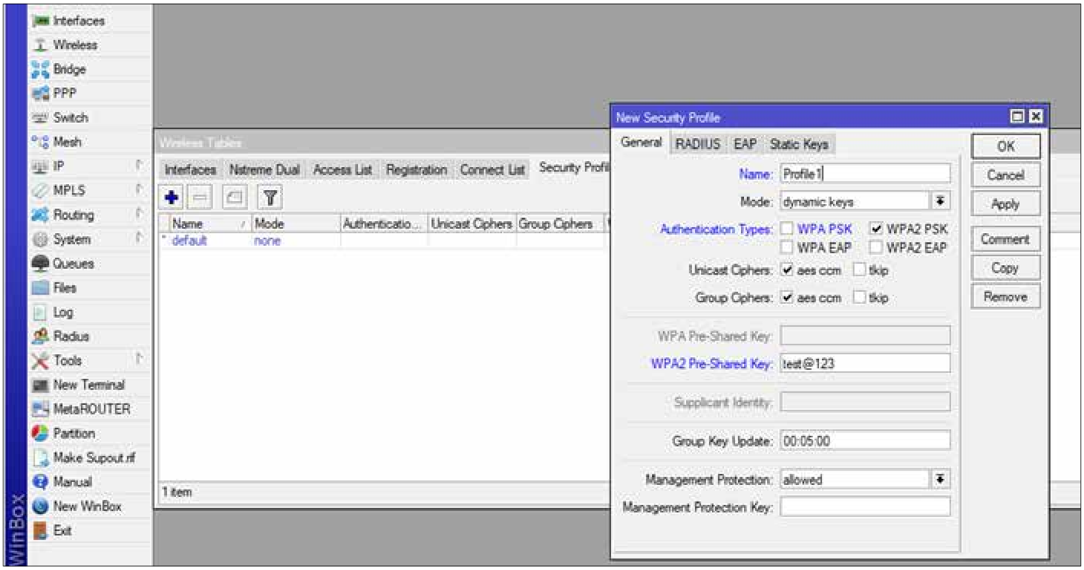
Session: 64:D1:54:77:6A:A0

Name	Type	Actual MTU	Tx	Rx	Tx Packet (p/s)	Rx Packet (p/s)	FP Tx	FP Rx	FP Tx Packet (p/s)	FP Rx Packet (p/s)
wlan1	Wireless (Atheros AR9...	1500	0 bps	0 bps	0	0	0 bps	0 bps	0	0

7. After adding the IP address, we are now ready to configure wireless interface. By default, wireless interfaces are disabled and we need to enable it before configuring it. Follow the above steps to enable the wireless interface.



Name	Mode	Authenticatio...	Unicast Ciphers	Group Ciphers	WPA Pre-Shared	WPA2 Pre-Shared...
* default	none				*****	*****



Name	Mode	Authenticatio...	Unicast Ciphers	Group Ciphers
* default	none			

Name: Profile1

Mode: dynamic keys

Authentication Types: □ WPA PSK ☑ WPA2 PSK □ WPA EAP □ WPA2 EAP

Unicast Ciphers: ☑ aes ccm □ tkip

Group Ciphers: ☑ aes ccm □ tkip

WPA Pre-Shared Key:

WPA2 Pre-Shared Key: test@123

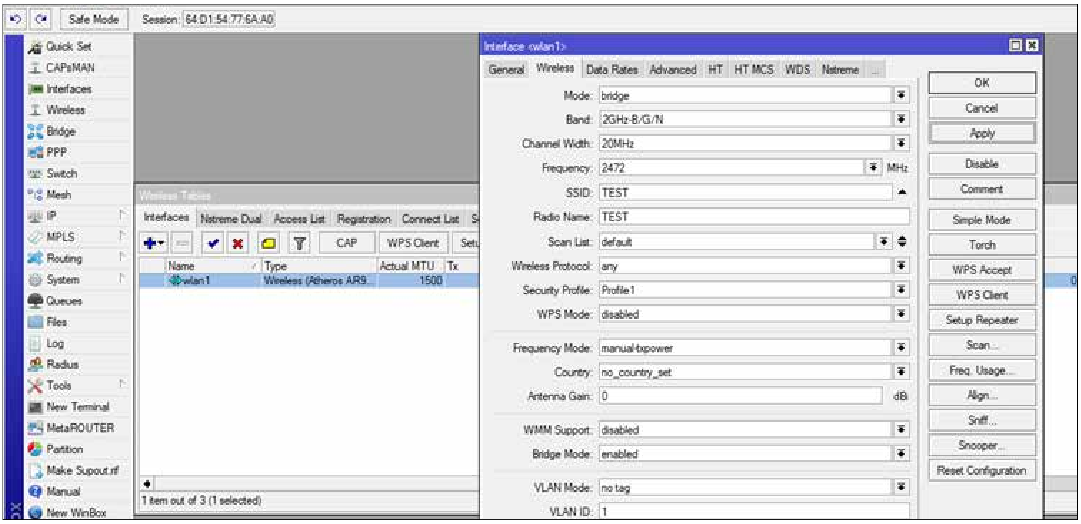
Supplicant Identity:

Group Key Update: 00:05:00

Management Protection: allowed

Management Protection Key:

8. After enabling the wireless interface, we need to create a security profile which will be used in association with our SSID to make it secure. Follow the above steps to create a security profile.



wlan1 Wireless (Atheros AR9... 1500

Mode: bridge
Band: 2GHz-B/G/N
Channel Width: 20MHz
Frequency: 2472 MHz
SSID: TEST
Radio Name: TEST
Scan List: default
Wireless Protocol: any
Security Profile: Profile1
WPS Mode: disabled
Frequency Mode: manual-txpower
Country: no_country_set
Antenna Gain: 0 dBi
WMM Support: disabled
Bridge Mode: enabled
VLAN Mode: no tag
VLAN ID: 1

These are the main steps as they define our wireless broadcasts. To learn the detailed descriptions of each option, you can refer to the product documentation website.

After configuring these options, we now have to make our devices secure. To do so, we can have an identity for our device to identify it uniquely in our network. It is also very important to assign login password for our device, which is by default left blank.

Go to, System -> Identity, a new window will appear where we can set a new identity for our device. Click OK after typing in a new identity.

It is utmost important to change the login password of our devices to make it secure from un-authorised physical access. Follow the above picture to change the login password.

Go to, System-> Password, type in the desired new password in the password dialogue box twice. Click on OK to confirm and exit.

Here we have seen the configurations of all the devices that are used on the Internet in a Box. Always notice and remember the physical layout and connections of wire used in the above concepts.

!

To view the corresponding video
on the course website, you can
scan the QR Code displayed here
or directly log in to the course
website http://lms.defindia.org

Video Duration: 1:16 Minutes

Earthing for Towers

When you install any metal pole on your roof, you are creating a lightning rod! Lightning can be very damaging, so we want to make sure we protect against it. It is important to note that if your house or building isn't the highest thing in the area - for instance, if there are tall trees close by or if there are other taller buildings around - your risk of actually being struck by lightning is extremely small.

Lightning protection is a must for any structure elevated above the surroundings. Lightening is a common enemy to wireless installations in high structures and must be prevented as far as it can.

There are two different ways lightning can strike or damage equipment: direct hits or induction hits.

Direct hits

Direct hits happen when lightning actually hits the tower or antenna. Induction hits are caused when lightning strikes near the tower.

Indirect hits

Induction currents (indirect hits) through nearby lightning strike can cause damage to outdoor radio equipment. It can be prevented by using surge protectors to vulnerable equipment and choosing radios that have a higher voltage rating. However, surge protectors do not protect the antenna, only the radio.

Protection from lightning

Keep this in mind, and don't panic about putting up an antenna mast! If you follow a few of these steps here you can protect yourself from damage to your home or electronics. Though lightning is dangerous, it is extremely unlikely to be struck. A more common problem is static build-up from the electric charge in the air during a lightning storm. This static can cause a charge to run down the cables from the roof and damage equipment in your house. We want to direct this charge into the ground, rather than into your electronics!

There are a few options for how to install lightning protection: a wire from the antenna mount to a grounding source or a surge arrester. How to decide? Generally, if you have a metal antenna mount on your roof that is over 5 feet tall, you will want to ground that using a long copper wire.

You have likely already used a surge arrester - they are sometimes built into multiple outlet power strips. They function by preventing a surge (quick build-up) of electrical energy from entering your appliances. This surge is shunted or directed to ground instead - either the large round pin on the wall plug (in the case of a power strip) or with a copper or aluminium wire if you are grounding outdoor equipment.

You want to install a surge arrester on the Ethernet cable that connects from the wireless Router on your roof to your indoor Access Point or computer. In order to do this, we will actually need to create two Ethernet cables: one that runs from the rooftop Router to the surge arrester, and one that runs from the arrester to the indoor unit. The surge arrester is grounded by running a #10 AWG copper or aluminium wire from a metal lug inside of the arrester to one of the grounding connections mentioned above. There are many models of surge arrester available but unfortunately aren't likely available in local hardware stores. We need special surge arrestors that mount outdoors and allow power from the Power over Ethernet adapter to reach the router.

To establish the earthing, you need the following equipment, if you are establishing the above-mentioned tower.

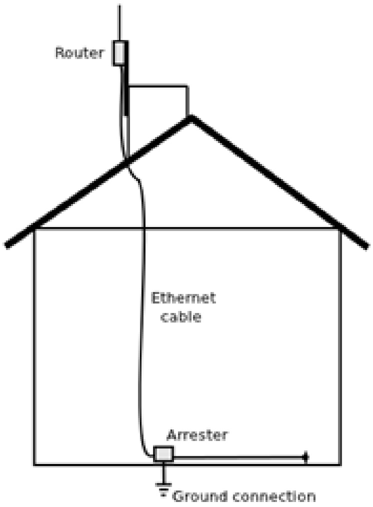


Figure 9 Example of showing earthing for tower

Table 3: Equipment list to establish the earthing

S.No.	Devices Names	Description
1	Lightning Arrestor with Insulator	
2	Chemical earthing copper bonded electrode	(50 mm X 3000mm)
3	Pit Box for one	
4	Copper shielded wire (16 MM)	90 Meter Bundle
5	Copper shielded wire (10 MM)	90 Meter Bundle
6	Copper shielded wire (2.5 MM)	90 Meter Bundle
7	Test link Box	
8	Surge Protector Device (SPD)	AC Single phase with neutral and earth
9	GI Strip	25 mm X 3

Summary

UNIT SUMMARY

In this unit, you learned how to establish the tower of 10 feet height for broadcasting the internet from your location. You also learned steps to configure the devices for broadcasting devices and doing earthing to protect your devices from lightning.

Reading

ADDITIONAL READING

Basics of IP and DNS

Wireless Networking In the Developing World, Chapter 6 - Networking

http://wndw.net/download/WNDW_Standard.pdf

Assessment

ASSESSMENT

Now that you have completed this unit, check your understanding of the concepts learned by responding to the following questions.

You can also take this assessment on the course website.

You can compare your response with the response displayed in the Ideal Responses section.

Question 1: What is the purpose of an IP address? Choose the correct answer from the following:

a. To identify the manufacturer of a device.
b. To identify the size of a device.
c. To identify a device to other devices in the network
d. To identify the exact location of a device.

Question 2: Sandeep has a 6-foot tall metal antenna mounted on his roof. Should he use earthing? Choose the correct answer from the following:

a. Yes, he should use earthing using a long copper wire.
b. No, he doesn't need earthing as the antenna is only 6-feet tall.

IDEAL RESPONSES

Answer 1: c. An IP address is an identifying number for a piece of network hardware. Having an IP address allows a device to communicate with other devices over an IP-based network like the internet.

Answer 2: a. He needs earthing as the antenna may be elevated above the surrounding structures and also because it is made of metal.

Unit

7

Secondary Infrastructure Setup

Introduction

Now, we can read the story of Monika who is ready to also set up secondary infrastructure.

Monika, now you know how to set up the primary infrastructure in your location to broadcast the internet services to your neighbours.
SECONDARY
INFRA
Yes, Raju. In the previous unit, you said that to extend my Internet services to Kabir chacha, we have to set up secondary infrastructure at his location.
That's right. We will now look at the equipment and process required for you to provide internet services at another location.
CPEs
WISP
TP-LINK
BRIDGE STATION MODE
BINATONE
AP-MODE
SECONDARY INFRASTRUCTURE
Sounds interesting. Let's start this unit on setting up the secondary infrastructure.

!

To view the corresponding video on the course website, you can scan the QR Code displayed here or directly log in to the course website http://lms.defindia.org

Video Duration: 0:35 Seconds

Outomes

In the unit on primary infrastructure, you learned how to set up the configuration of access points. This unit will cover details of setting up secondary infrastructure in other locations. Upon completion of this unit you will be able to:

- Set up Client Premises Equipment (CPE).
- Describe the role of devices used as CPE.
- Configure devices at the client location.
- Assemble devices at the client location

Terminology

Signal to Noise Ratio: A measure of how much useful information there is in a system, such as the Internet, as a proportion of the entire contents.

Client Premises Equipment: Any terminal and associated equipment located at a subscriber's premises and connected with a carrier's telecommunication circuit at the demarcation point ("demarc").

Bridge/Station Mode A networking device that is used to connect two different types of networks.

Client Site Installations

In the unit on primary infrastructure, we established Access Point (AP) devices at the location from where the Internet will be broadcast. For a sustainable network, it is important to ensure proper installation at the client site. Let us now learn about configuring devices on the client side.

Locating the installation site at the client location

While you may find several suitable spots for installing CPE, the selection of the installation spot should be done carefully. Some of the considerations for selecting an installation spot are described below:

1. It should be at the highest spot available on the roof. Even if there is a proper signal at a lower spot, always select the highest spot available.
2. The minimum required SNR (Signal to Noise Ratio) is 22-25. You can calculate the SNR by deducting the signal value from the noise floor.

> Example
>
> Noise floor on frequency 5220 = -101
>
> Signal at a CPE 6 KMs away from tower = -70
>
> SNR = Noise floor – Signal = -101-(-70) = 31. 31

3. While mounting the CPE, make sure it is far away from any electric wires to avoid Electro Magnetic Interference. Symptoms of interference may include a rapid change in SNR.
4. While mounting the CPE, make sure it is far away from dense trees or plants. Dense trees or plants absorb most of the frequency waves resulting in loss of data packets even if you get a proper signal.
5. Windy areas should be avoided. If not, mount the CPE over a dense wooden or metal rod to prevent movement when the wind blows. The rod on which the CPE is mounted plays a significant role in the proper functioning of the client's connection. If the rod is loose or moves when the wind blows, it will result in retransmission timeouts of the packets.

Example

Mount the CPE over a 1-inch, light-weight PVC pipe, leaving a foot at the top to mount the CPE. Beyond the empty area at the top, tie GI wires and stretch and tie them along three sides on the roof to avoid any movement during strong winds.

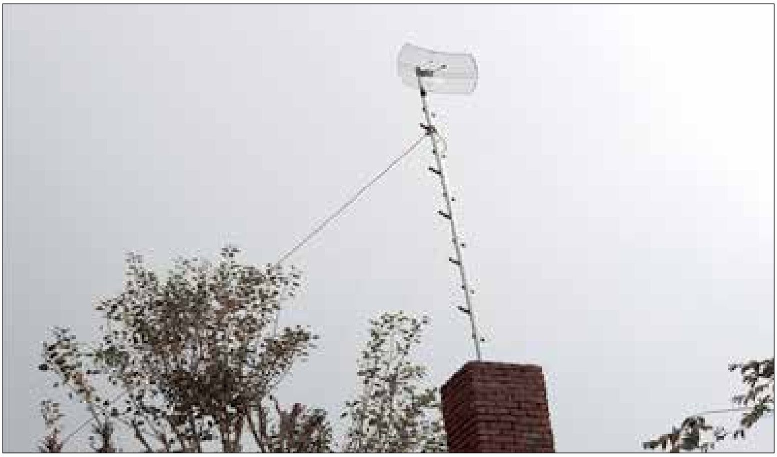


Figure 10: PVC pipe with GI wires

Installation Modes

There are two major installation modes available for CPEs - Bridge/Station Mode and Router Bridge/WISP Client Router Mode. It is important to select the most suitable mode depending on the situation. Let us study each mode in detail.

Bridge/Station Mode

A bridge is a networking device that is used to connect two different types of network. For example, connecting a wireless network to a wired network. Bridges are transparent to the network; these devices cannot be seen using any network diagnostic tool.

In this mode, WLAN and Ethernet of CPE, both work in bridge mode. This mode eliminates an extra hop (router) in the network, which may (or may not) include extra latency to the network. Please note, routers include extra latency to the network because they need extra time to de-capsulate and again encapsulate a data packet, and then forwards it to the desired destination. While bridge simply forwards the data packet from one interface to another.

Scenario 1: This mode is suited for setup at a client who intends to use only a DVR. This way, we will have to assign our root network's IP over DVR's LAN. It makes us easy to forward the desired ports for bringing the DVR online.

Scenario 2: We can also use this mode if the client is using or has bought a wireless router. This way we can assign our root network's IP over Wireless Router's WAN (Wireless Area Network) port to avoid extra hop. Remember, assigning our root network's IP over client's owned devices will leave the setup open to being interfered with. Since the client owns the device, we need to inform the client that he or she should not make any changes to that device without informing us in advance.

Router Bridge/WISP Client Router Mode

A router is a networking device that is used to route the network traffic. It is also used to implement security to the network like implementing Firewall and NATting.

This mode is the rather secure and preferred mode of implementation, as we assign our root network's IP on our CPE, which will not be tampered with without our knowledge.

In this mode, WLAN of our CPE works in Bridge mode and Ethernet interface of the CPE works in Router mode, making it easy to change device/PC/Laptop below that CPE.

This mode is mostly preferred if the client is using a PC/Laptop directly below our CPE, the router is running on Ethernet of our CPE which dynamically assigns IPs to devices connected below it. It allows our clients to change their device anytime they want.

Configuring CPE

In this Unit, we will see both device companies – TP Link and Ubiquity AirGrid details and its configuration. Devices with their roles in detail are given below:

TP Link 5210 2.4 GHz Radio

It has 3 major modes:

1. AP
2. AP Router
3. WISP Client Router

Mode 1 - AP: In this mode, this device works as transparent AP Bridge if its WLAN is broadcasting an SSID. DHCP won't work in this mode. If the Wireless of the device is set to Client, this device will work as a transparent CPE. If the wireless of the device is set to Repeater or Universal Repeater, this device will rebroadcast the SSID that it is connected to and it will also work as a transparent CPE.

Mode 2 - AP Router: In this mode, the WLAN of this device works as a router while the LAN/Ethernet port of the device works as input for Internet connectivity.

Note: We need to enable SSID and DHCP of the device for it to work.

Mode 3 - WISP Client Router: In this mode, the WLAN of the device works as Client/Station/CPE while the LAN/Ethernet port of the device works as Router.

Binatone CPE is the device works exactly the same as TP Link 5210, the only difference is that we can enable it's radio's broadcast while it works in WISP Client mode.

Ubiquity's AirGrid M5 HP

It is the most sophisticated device that we use for installation at a client site. It is very much stable and provides proper connectivity.

Though it's configuration is a bit tricky and complicated, mastering this device is very useful.

We need to configure it's wireless and network/LAN separately and they are always interdependent.

Mode 1, configuring the device in complete transparent bridge mode

As we have already discussed the bridge and router modes of the devices, hence thus, we can refer above. To configure the device in complete transparent bridge mode, we need to configure the wireless mode of the device as Station, and then configure the network/LAN of the device to Bridge.

Mode 2, configuring the device in WISP Client Router/Station Router mode

To configure the device in this mode, we need to configure the wireless of the device to Station and network/LAN of the device to Router modes respectively.

As this document focuses mainly on 'TO DO's 'while setting up CPE at a client site, we have not touched configuration parts in detail. You will definitely be provided with a proper training before visiting the field. That is when you will learn most of the configurations. Also, there is another booklet that deals in configuring each and every device in details with a screenshot.

Configuring Client Premises Equipments (CPEs)

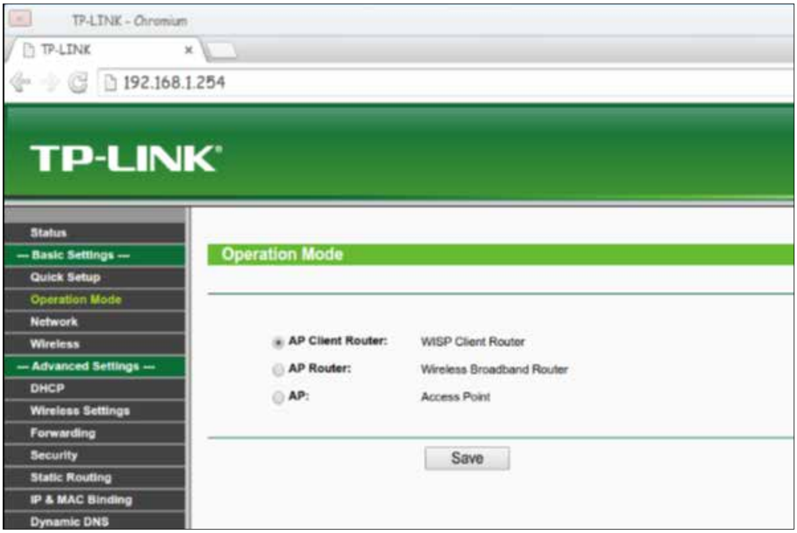
In order to configure a radio device, we need to assign the IP address of the same series to our laptops. This topic has already been discussed. Here we will start with CPE configuration.

The configuration of TP Link 5210 Radio

TP Link 5210 2.4 GHz Radio is a most suitable device for wireless connection. We already had discussed its modes of configuration. Here we are discussing how to configure it in different Operational modes.

Mode 1: AP Client Router

In this mode, the WLAN of the device works as Client/Station/CPE while the LAN/Ethernet port of the device works as Router.



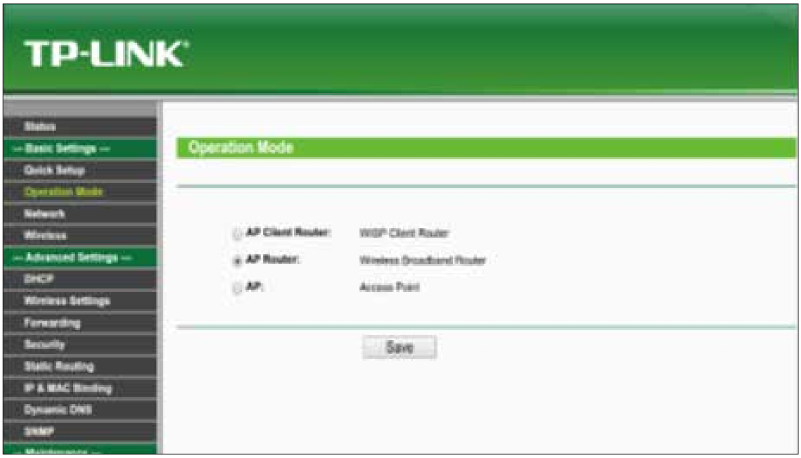
Operation Mode

● AP Client Router: WISP Client Router
○ AP Router: Wireless Broadband Router
○ AP: Access Point

Mode 2: AP Router

In this mode, the WLAN of this device works as a router while the LAN/Ethernet port of the device works as input for Internet connectivity. Here we need to enable SSID and DHCP.

By enabling DHCP, it will give out IP addresses to the connected device of its own network that makes it easy to change connected device.

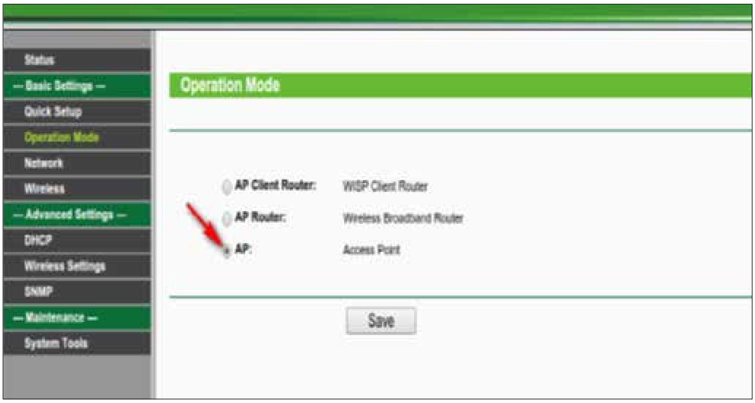


Operation Mode

○ AP Client Router: WISP Client Router
● AP Router: Wireless Broadband Router
○ AP: Access Point

Mode 3: AP

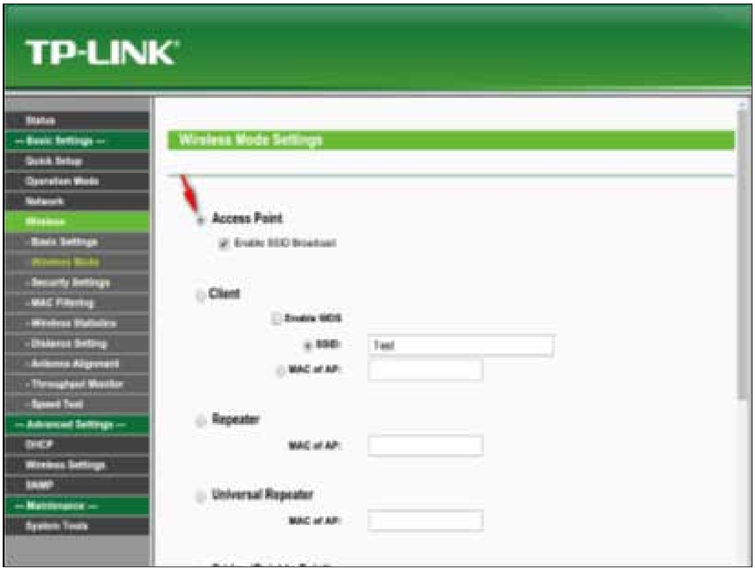
In this mode, TP Link provides a wireless connection to other devices by using Wi-Fi. It's WLAN and Ethernet port both work as LAN ports and it works as transparent AP bridge (i.e. It can't provide IP of its network).IP will be given by ISP's side. It will work according to the mode of its wireless mode.



Operation Mode

○ AP Client Router: WISP Client Router
○ AP Router: Wireless Broadband Router
● AP: Access Point

Scenario 1 Access Point: - If the wireless mode is Access Point, then stations or AP clients can access it. It will broadcast an SSID but will not be able to assign an IP address on its own.



Wireless Mode Settings

● Access Point
☑ Enable SSID Broadcast

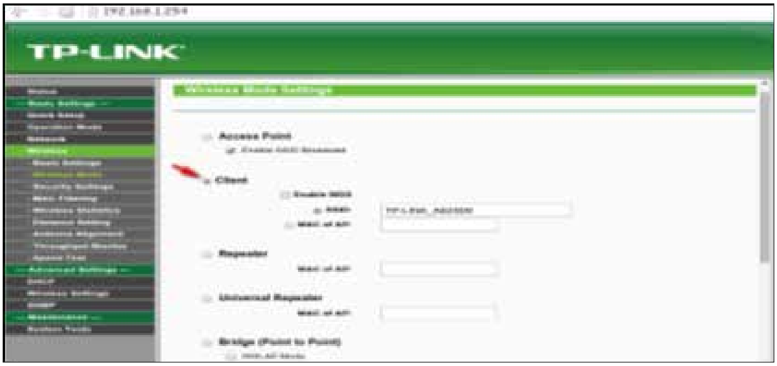
○ Client
□ Enable WDS
● SSID: Test
○ MAC of AP:

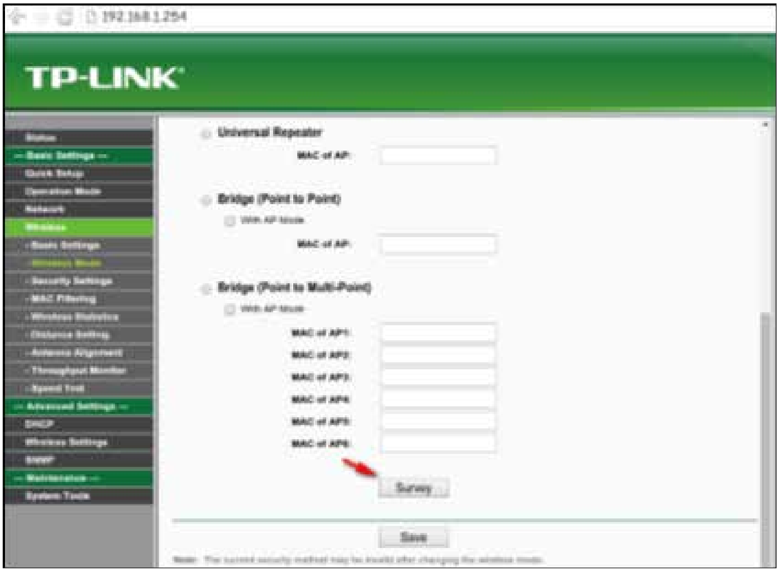
○ Repeater
MAC of AP:

○ Universal Repeater
MAC of AP:

Scenario 2 Client: - If the wireless mode is Client, it will work as a wireless station. Apart from that, some key points are described below.

After selecting Operation mode as AP, browse to Wireless->Wireless Mode. Click on Site survey, you will find it at the bottom of the page. As you click this link, a new page will open where you can select the desired SSID. Please note, beside SSID, you will see the signal of the respective SSID. Anything over 20 dB is a workable signal.

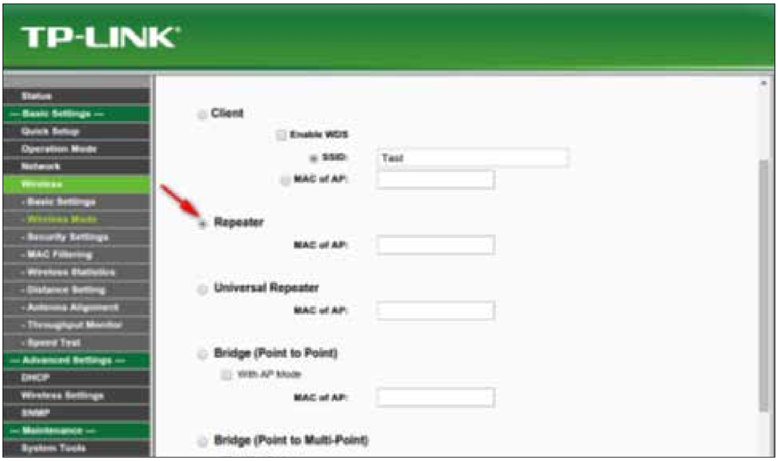




SSID- SSID is the name by which we want to access it.

MAC of AP- With this option, we can lock our CPE/Client/Station device with MAC of remote AP device.

Scenario 3 Repeater: - If the wireless mode is repeater it just re-broadcast the SSID. This mode is used to enhance the area of access by using the same SSID and the CPE will transparent. Please note, only one device can connect to the repeated signal if the device is configured as a repeater.



○ Client

□ Enable WDS

● SSID: Test

○ MAC of AP:

● Repeater

MAC of AP:

○ Universal Repeater

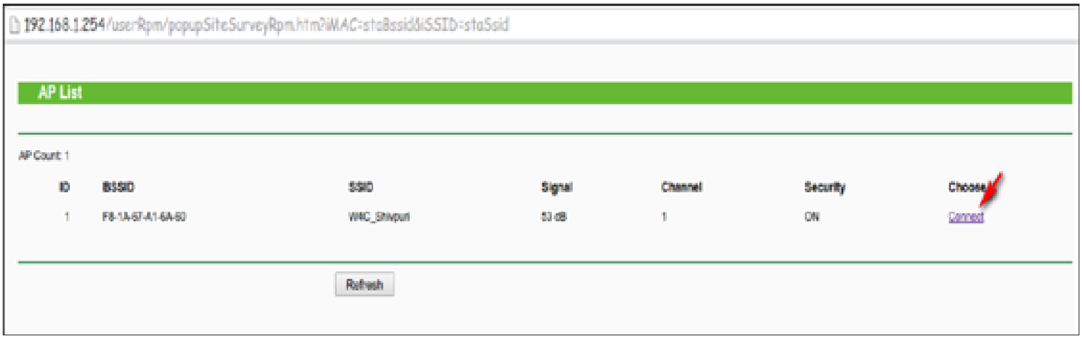
MAC of AP:

○ Bridge (Point to Point)

□ With AP Mode

MAC of AP:

○ Bridge (Point to Multi-Point)



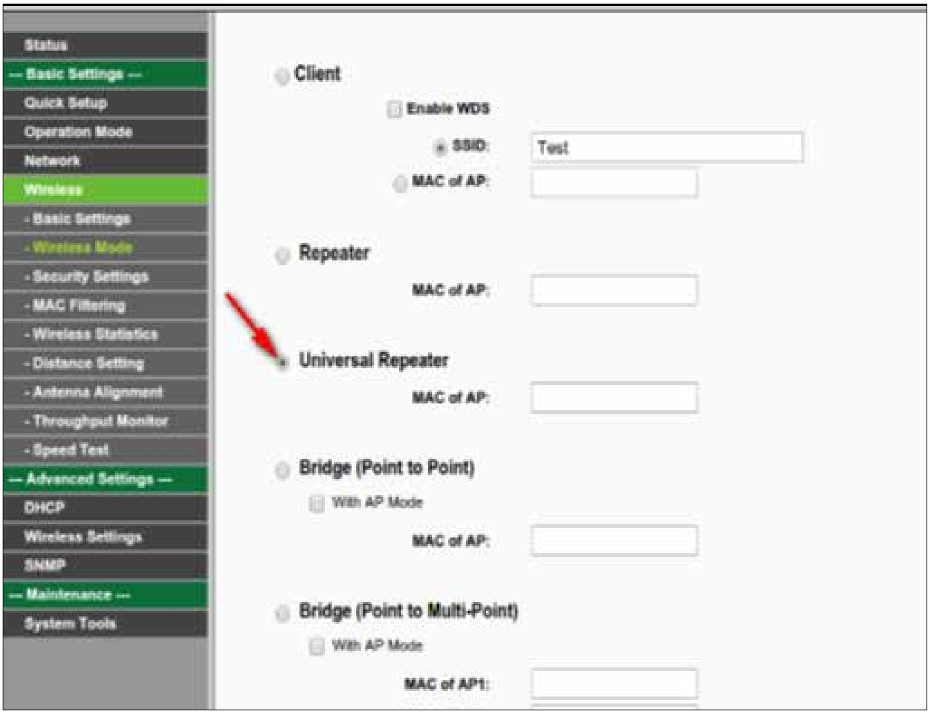
192.168.1.254/userRpm/popupSiteSurveyRpm.htm?MAC=staBssid&SSID=staSsid

AP List

AP Count: 1

ID	BSSID	SSID	Signal	Channel	Security	Choose
1	F8-1A-67-A1-6A-60	WMC_Shivpuri	53 dB	1	ON	Connect

Scenario 4 Universal Repeater: It is similar to repeater mode; the only difference is that Repeater connects only one device at a time, while Universal repeater can connect multiple devices to the repeated signal at the same instance of time.



○ Client

□ Enable WDS

● SSID: Test

○ MAC of AP:

○ Repeater

MAC of AP:

● Universal Repeater

MAC of AP:

○ Bridge (Point to Point)

□ With AP Mode

MAC of AP:

○ Bridge (Point to Multi-Point)

□ With AP Mode

MAC of AP1:

!

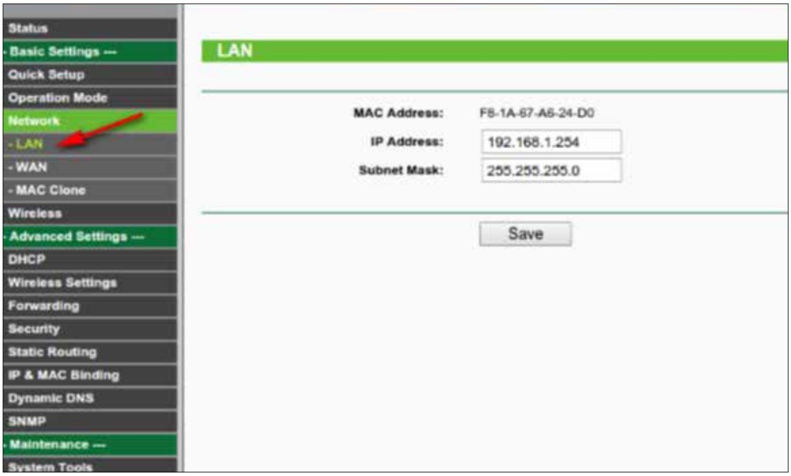
To view the corresponding video on the course website, you can scan the QR Code displayed here or directly log in to the course website http://lms.defindia.org

Video Duration: 2:12 Minutes

Network:

To set up the network, there are different modes - LAN, WAN, MAC Clone and Wireless.

LAN

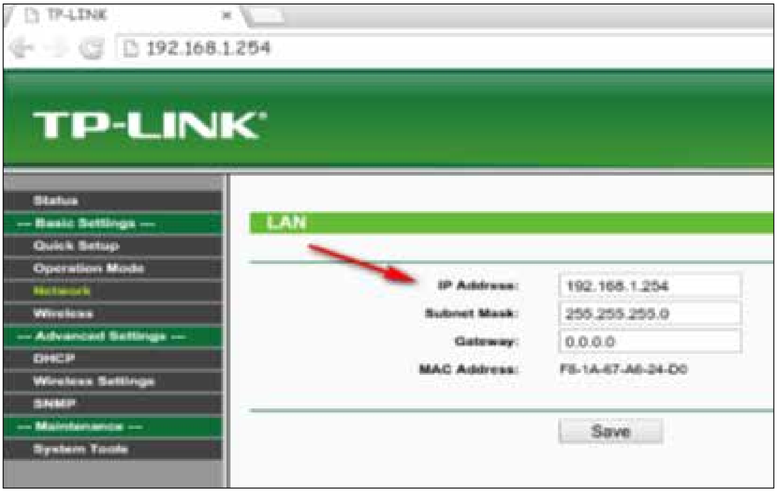


MAC Address: F8-1A-67-A6-24-D0

IP Address: 192.168.1.254

Subnet Mask: 255.255.255.0

Here we change IP Parameters for Router/AP mode (e.g. IP Address, Subnet mask). This is the IP by which we log onto the Router. This also defines the Network mask for the DHCP.



IP Address: 192.168.1.254

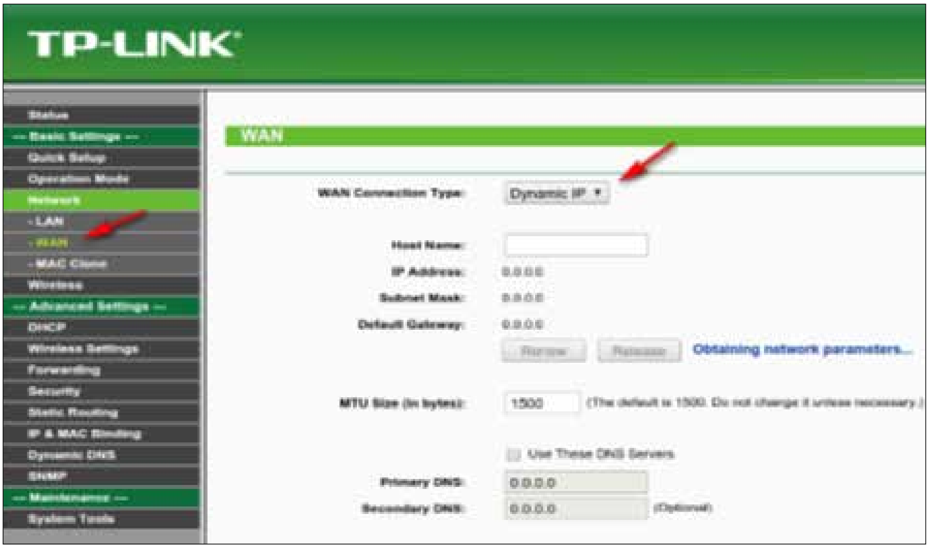
Subnet Mask: 255.255.255.0

Gateway: 0.0.0.0

MAC Address: F8-1A-67-A6-24-D0

WAN

If the ISP is running DHCP server, then it automatically provides the IP, Subnet mask, Gateway, Primary and Secondary DNS.



WAN

WAN Connection Type: Dynamic IP

Host Name:

IP Address: 0.0.0.0

Subnet Mask: 0.0.0.0

Default Gateway: 0.0.0.0

Obtaining network parameters...

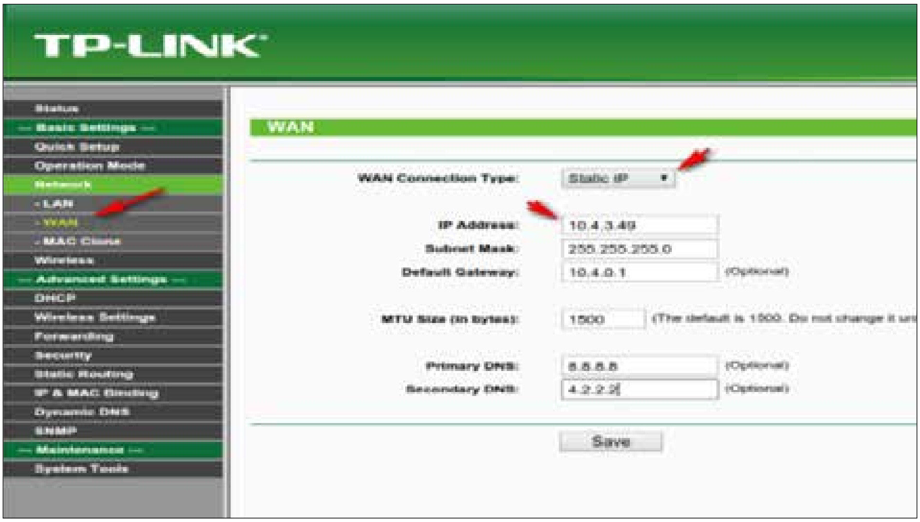
MTU Size (in bytes): 1500 (The default is 1500. Do not change it unless necessary.)

□ Use These DNS Servers

Primary DNS: 0.0.0.0

Secondary DNS: 0.0.0.0 (Optional)

If the ISP is not running a DHCP server, then we have to provide all those parameters manually.



WAN

WAN Connection Type: Static IP

IP Address: 10.4.3.49

Subnet Mask: 255.255.255.0

Default Gateway: 10.4.0.1 (Optional)

MTU Size (in bytes): 1500 (The default is 1500. Do not change it un

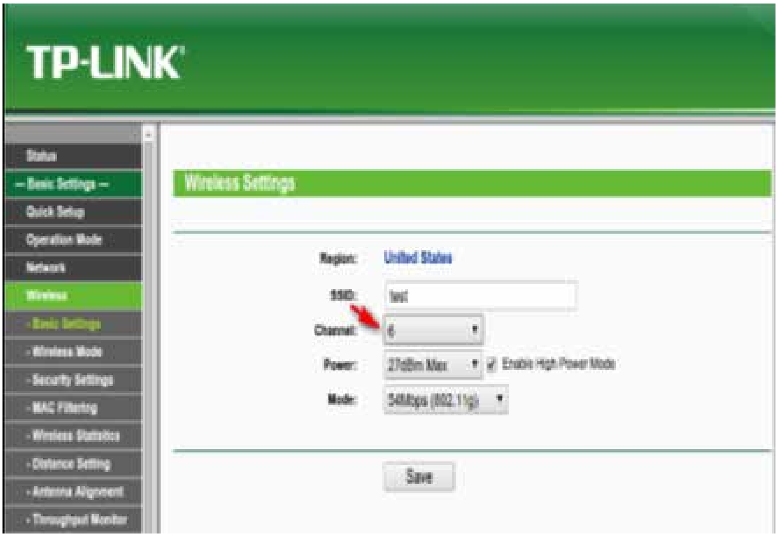
Primary DNS: 8.8.8.8 (Optional)

Secondary DNS: 4.2.2.2 (Optional)

Wireless: We should change wireless setting only if it is working as AP/ AP Router mode.

Basic Setting

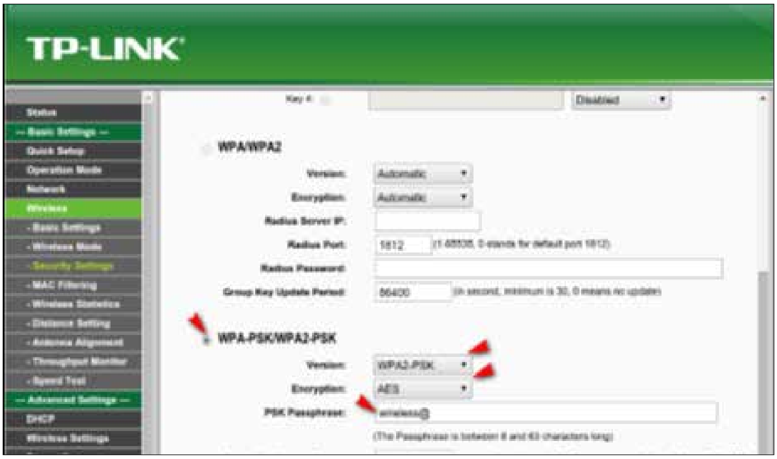
Here only SSID and Channel need to be changed. Usually, Channel is set to 1, 6 or 11 or default (automatic).



Region: United States
SSID: test
Channel: 6
Power: 27dBm Max ☑ Enable High Power Mode
Mode: 54Mbps (802.11g)

Security Setting

Here we secure our network. We generally use WPA2-PSK and encrypted by AES and also prove a password



Key 4: ○ Disabled

○ WPA/WPA2

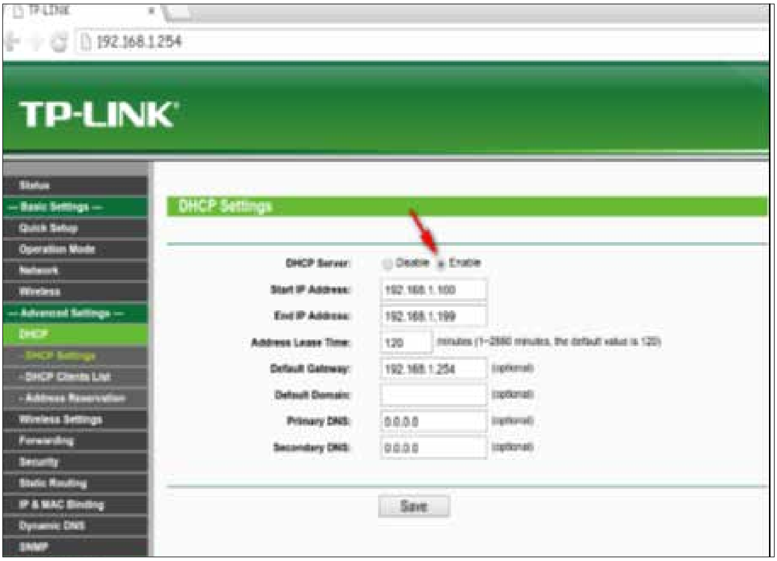
Version: Automatic
Encryption: Automatic
Radius Server IP:
Radius Port: 1812 (1-65535, 0 stands for default port 1812)
Radius Password:
Group Key Update Period: 86400 (in second, minimum is 30, 0 means no update)

● WPA-PSK/WPA2-PSK

Version: WPA2-PSK
Encryption: AES
PSK Passphrase: wireless@
(The Passphrase is between 8 and 63 characters long)

DHCP

DHCP is enabled if the device is working in Wireless Broadband Router (AP Router) and WISP Client Router.



DHCP Server: ○ Disable ● Enable

Start IP Address: 192.168.1.100

End IP Address: 192.168.1.199

Address Lease Time: 120 minutes (1~2880 minutes, the default value is 120)

Default Gateway: 192.168.1.254 (optional)

Default Domain: (optional)

Primary DNS: 0.0.0.0 (optional)

Secondary DNS: 0.0.0.0 (optional)

!

To view the corresponding video on the course website, you can scan the QR Code displayed here or directly log in to the course website http://lms.defindia.org

Video Duration: 1:46 Minutes

The configuration of Ubiquity's AirGrid M5 HP

It is the most sophisticated device that we use for installation at a client site. It is very much stable and provides proper connectivity. It is a highly precise CPE device which works at a range up to 10km. It provides two modes of working, Router/Station mode and transparent Bridge mode. In it, we need to configure Wireless and Network both separately.

Station Bridge Mode: In Bridge mode, it works as a transparent CPE device. In this mode, it can't provide IP addresses that is why it is necessary to have a running DHCP server at ISP side. We can also provide static IP address to the node connected to the CPE device

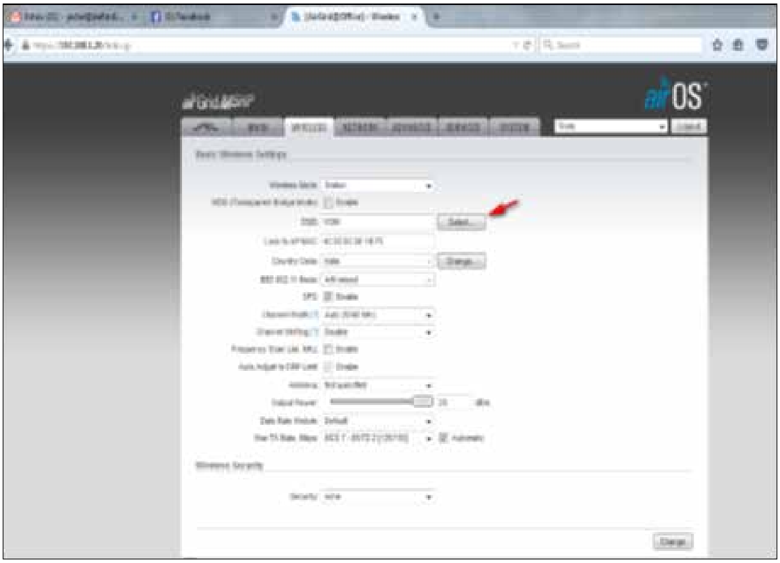
Network Setting

Network Mode- Bridge

Wireless Setting

Wireless mode – Station

After configuring all of these we survey the site and choose the SSID of the AP and lock it. Or we can scan once we have configured wireless tab.



Basic Wireless Settings

Wireless Mode: Station

WDS (Transparent Bridge Mode): □ Enable

Frequency Scan List, MHz: □ Enable

Auto Adjust to EIRP Limit: □ Enable

Output Power: dBm

Data Rate Module: Default

Max TX Rate, Mbps: ☑ Automatic

Wireless Security

Security: none

Router Mode: This mode is most preferred if the client is using a PC/Laptop directly below our CPE, as the router is running on Ethernet of our CPE which dynamically assigns IPs to devices connected below it. It allows our clients to change their device anytime they want.

Network Setting

Network Mode-Router

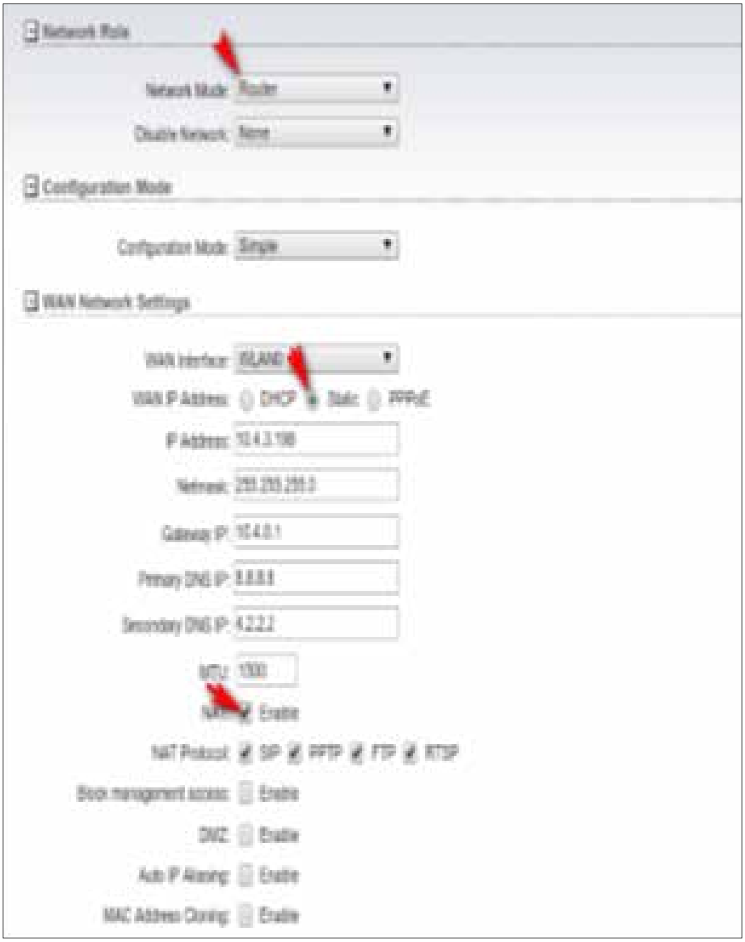
Wireless Setting

Wireless Mode- Station

Provide static IP, Netmask, Gateway, Primary and Secondary DNS. Enable NAT.

LAN Network Setting

Change LAN IP if required. Then enable DHCP server and update start and end range. And enable UPnP. After configuring all of these we survey the site and choose the SSID of the AP and lock it.



Network Role

Network Mode: Router

Disable Network: None

Configuration Mode

Configuration Mode: Simple

WAN Network Settings

WAN Interface: WLAN0

WAN IP Address: ○ DHCP ● Static ○ PPPoE

IP Address: 10.4.3.198

Netmask: 255.255.255.0

Gateway IP: 10.4.0.1

Primary DNS IP: 8.8.8.8

Secondary DNS IP: 4.2.2.2

MTU: 1500

NAT: ☑ Enable

NAT Protocol: ☑ SIP ☑ PPTP ☑ FTP ☑ RTSP

Block management access: □ Enable

DMZ: □ Enable

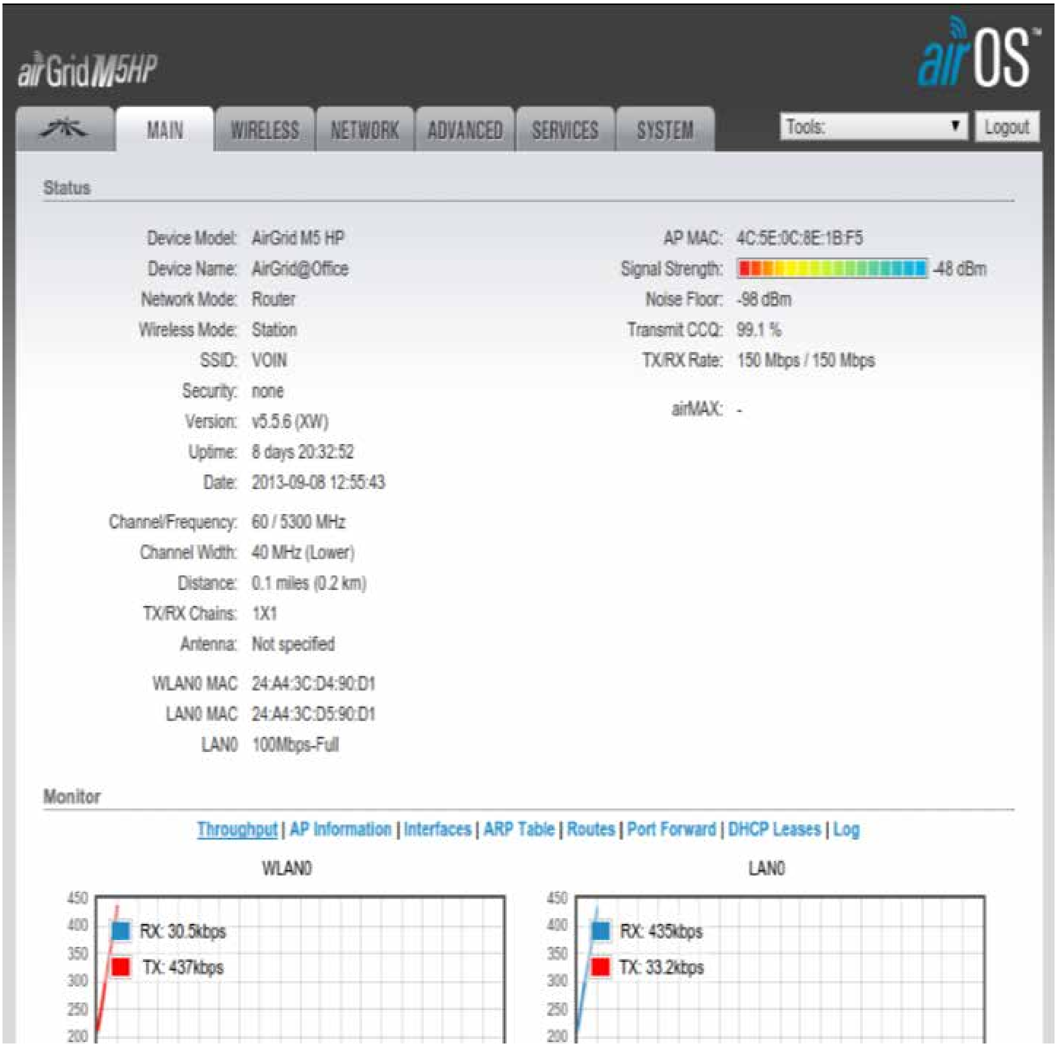
Auto IP Aliasing: □ Enable

MAC Address Cloning: □ Enable

At last check in Main option. Observe Signal strength and Noise Floor.

Transmit CCQ should stable and not frequently changing.

Tx/Rx reflects transmit and receive rate.



Status

Device Model: AirGrid M5 HP
Device Name: AirGrid@Office
Network Mode: Router
Wireless Mode: Station
SSID: VOIN
Security: none
Version: v5.5.6 (XW)
Uptime: 8 days 20:32:52
Date: 2013-09-08 12:55:43

Channel/Frequency: 60 / 5300 MHz
Channel Width: 40 MHz (Lower)
Distance: 0.1 miles (0.2 km)
TX/RX Chains: 1X1
Antenna: Not specified

WLAN0 MAC 24:A4:3C:D4:90:D1
LAN0 MAC 24:A4:3C:D5:90:D1
LAN0 100Mbps-Full

AP MAC: 4C:5E:0C:8E:1B:F5
Signal Strength: -48 dBm
Noise Floor: -98 dBm
Transmit CCQ: 99.1 %
TX/RX Rate: 150 Mbps / 150 Mbps

airMAX: -

Monitor

Throughput | AP Information | Interfaces | ARP Table | Routes | Port Forward | DHCP Leases | Log

!

To view the corresponding video on the course website, you can scan the QR Code displayed here or directly log in to the course website http://lms.defindia.org

Video Duration: 1:59 Minutes

Summary

UNIT SUMMARY

In this unit, you learned about client site installation and devices that are required to be used at the client location. You also learned how to choose the installation location at the client site.

In addition, you also learned the role of devices manufactured by – Ubiquity Airtgrid and TPLink. You also learned the process for configuring these devices.

Assessment

ASSESSMENT

Now that you have completed this unit, check your understanding of the concepts learned by responding to the following questions.

You can also take this assessment on the course website.

You can compare your response with the response displayed in the Ideal Responses section.

Question 1: Anthony wants to mount CPE at a site which has some electric wires nearby. But it's okay for him to install the CPE at that location. True or False?

a. True
b. False

Question 2: A networking device is used to connect two different types of network. Which mode is this?

a. Station Mode
b. Router Bridge Mode

IDEAL RESPONSES

Answer 1: b. While mounting the CPE, it is important to ensure it is far away from any electric wires to avoid Electro Magnetic Interference.

Answer 2: a. The Station Mode or Bridge Mode is a networking device that is used to connect two different types of network. For example, connecting a wireless network to a wired network.

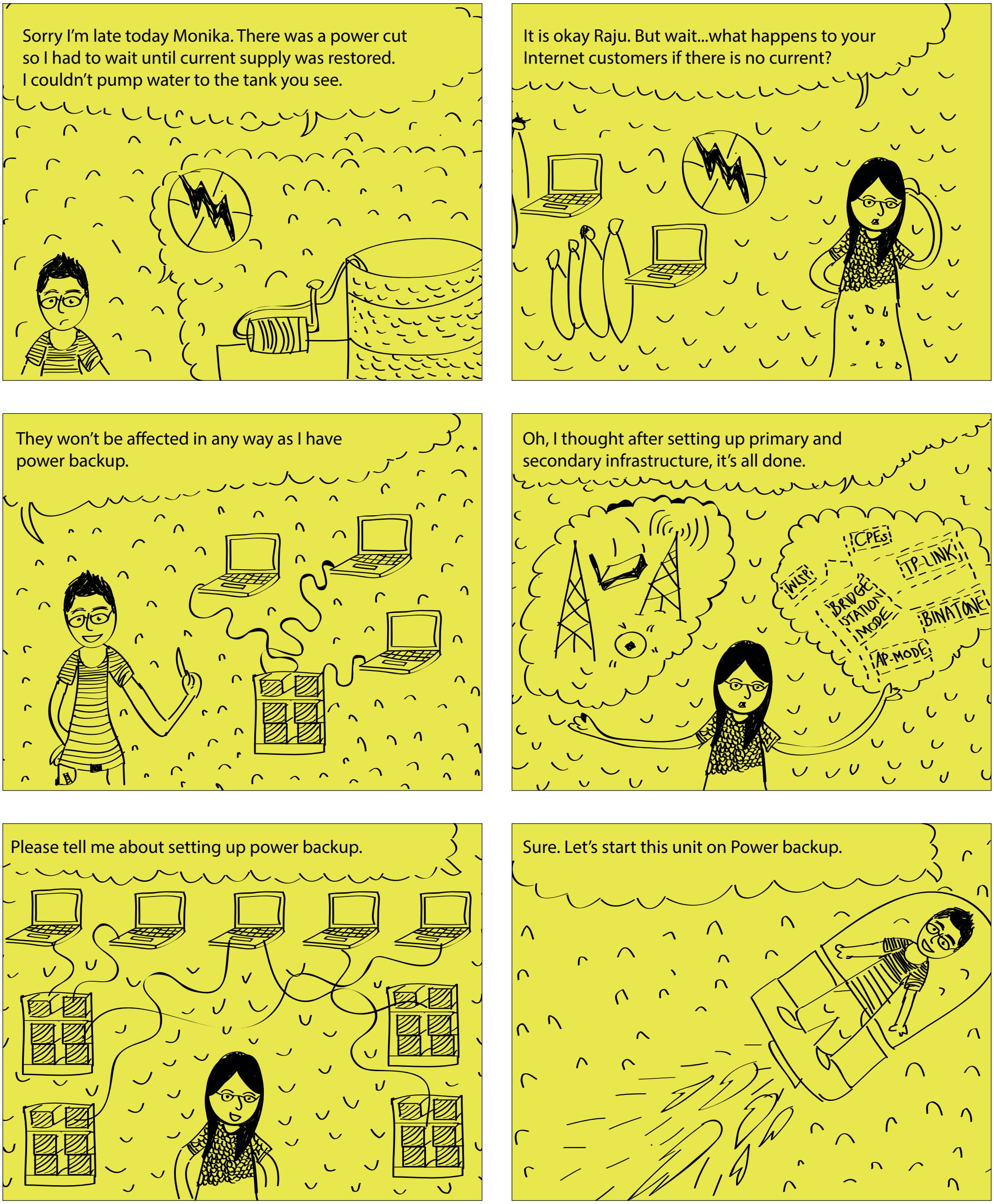
Unit

8

Power Backup

Introduction

After setting up the network, read the story of Monika learning power backup.


Sorry I'm late today Monika. There was a power cut so I had to wait until current supply was restored. I couldn't pump water to the tank you see.
It is okay Raju. But wait...what happens to your Internet customers if there is no current?
They won't be affected in any way as I have power backup.
Oh, I thought after setting up primary and secondary infrastructure, it's all done.
WISP
CPEs
TP-LINK
BRIDGE STATION MODE
BINATONE
AP-MODE
Please tell me about setting up power backup.
Sure. Let's start this unit on Power backup.

!

To view the corresponding video on the course website, you can scan the QR Code displayed here or directly log in to the course website http://lms.defindia.org

Video Duration: 0:34 Seconds

Outomes

It is important to have power backup for the network to ensure uninterrupted services. This unit describes various types of power backup and procedures for setting it up.

Upon completion of this unit you will be able to:

» Define what power backup is.
» Setup electricity backup.
» Setup solar power backup.
» Use UPS for power backup

ABC

Terminology

UPS: An uninterruptible power supply or uninterruptible power source (UPS) is an electrical apparatus that provides emergency power to a load when the input power source or mains power fails

AVR: The automatic voltage regulator (AVR) is used to regulate the voltage. It takes the fluctuating voltage and changes them into a constant voltage.

Alternating current: An electric current which periodically reverses direction.

Direct current: An electric current which flows in one direction.

Definition of power backup

A backup battery provides power to a system when the primary source of power is unavailable. Backup batteries range from small single cells to retain clock time and date in computers, up to large battery room facilities that power uninterruptible power supply systems for large data centers. Small backup batteries may be primary cells; rechargeable backup batteries are kept charged by the prime power supply.

Introduction to Power Backup

In many developing countries, the demand for electricity is higher than what the provider can supply. So there may be frequent power cuts by the provider. Also, if there are power fluctuations, electrical equipment may be damaged.

Given these challenges, careful consideration is required before deciding on a power supply for equipment. An important factor for consideration is the distance of the tower from a power source and its accessibility for troubleshooting. There are several instances where network engineers have reported burnt routers due to power fluctuations. It may take hours of travel to troubleshoot distant links which have been drained of their power after a power line went down.

If the equipment is going to be placed on a rooftop or within a reasonable distance, powering the equipment with electricity from the grid might not be so complicated. You may need to obtain the power company for permission to hook on to the network by digging down an extension cable to the grid. It's possible that any additional digging or cable laying for the connection to the grid has to be done by the power company.

However, if a tower is very far from the power grid or if digging is not feasible, we should consider alternate sources of power such as UPS, windmills or solar panels. When we budget for power, we should not only budget for the equipment but also for the cost of installation, transportation and yearly maintenance.

Note about cables: When dealing with cables (data or electricity), it is important to consider proper installation methods to prevent damage by pests or the weather and theft.

Using UPS for Backup

To ensure the 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.

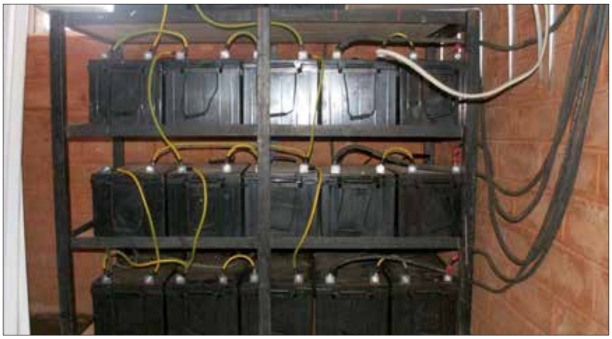


Figure 11: Batteries and battery chargers

The solution to the unstable power is to add batteries, battery chargers, AVR (automatic voltage regulator), and inverters to those nodes 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 the cheapest part of the system and easier to replace than radio equipment.

Any inverter UPS from a reputed company like Mikrotek or Luminous with 500 Watts power and Exide Battery of 100 aH can be used. An Inverter UPS is a must at the centre where leased line is coming in. However for better network performance, every centre should have a power backup.

There are off-the-shelf 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. The problem with a standard UPS is that surge voltage may pass through to the equipment. An online UPS converts the grid AC to DC and then rectifies it back to AC. Since the power in the output plugs of the UPS is never direct from the power grid the power surge does not reach the equipment.

Solar Backup

Solar power although almost trouble-free is comparatively expensive. Bearing the capital costs for these relays ourselves stretches a challenging economic proposition even further while having clients pay the full costs for a relay limits the type of clients who can avail the connections. A solar backup should be considered after evaluating all the pros and cons based on your plans and potential revenue.

Bearing the capital costs for these relays ourselves stretches a challenging economic proposition even further, while having clients pay the full costs for a relay limits the type of clients who can avail our connections.

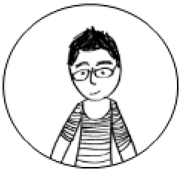
UNIT SUMMARY

Summary

In this unit, you learned about some of the options available for power backup such as UPS and solar power. You also learned how having power backup can provide uninterrupted services to clients and prevent equipment from being damaged by power surges.

Assessment

ASSESSMENT



Now that you have completed this unit, check your understanding of the concepts learned by responding to the following questions.

You can also take this assessment on the course website.

You can compare your response with the response displayed in the Ideal Responses section.

Question 1: Sania is trying to decide what power supply she should use for a tower which is on a hill about 6 km from her main centre. She has just started her Internet business and has about 11 customers. Which of the following is the most suitable power backup option for Sania?

a. Main grid supplied by the electricity board in her district
b. Solar power
c. Windmills
d. UPS

Question 2: Which of the following are benefits of having a UPS power backup? Select the two correct options.

a. Prevents equipment damage from power surges
b. Reduces the cost of Internet plans from the ISP
c. Ensures continuity of services in case of a power cut
d. Increases the range of the transmission of data

IDEAL RESPONSES

Asnwer 1: d. Solar power or Windmills may be an expensive investment at this stage. A UPS can protect Sania's equipment from power surges.

Answer 2: a, c. UPS power backup prevents equipment damage from power surges as it converts the grid AC to DC and then rectifies it back to AC. It also ensures continued power supply as it has stored power in its batteries.

Unit

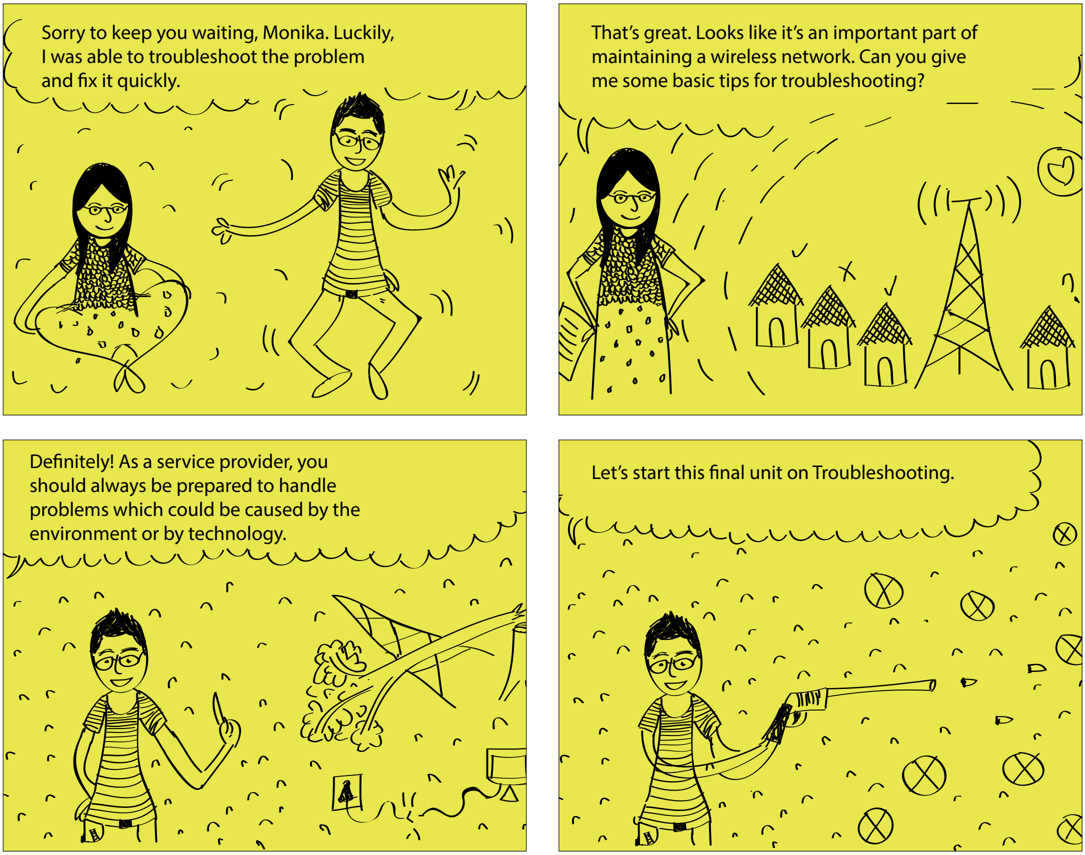
9

Troubleshooting

Introduction

After learning power backup, read the story of Monika who will be learning troubleshooting.

Give me one minute Monika, I have to take this call.
Hi Sushma. This is a pleasant surprise.
Bhaiyya, something is wrong. There's no internet for the past 10 minutes.
@
e
Sorry about that Sushma, I will just troubleshoot the problem and get it working. Bye.
Bhaiyya, something is wrong. There's no internet for the past 10 minutes.
Sorry about that Sushma, I will just troubleshoot the problem and get it working. Bye.
12
3
6
9


Sorry to keep you waiting, Monika. Luckily, I was able to troubleshoot the problem and fix it quickly.
That's great. Looks like it's an important part of maintaining a wireless network. Can you give me some basic tips for troubleshooting?
Definitely! As a service provider, you should always be prepared to handle problems which could be caused by the environment or by technology.
Let's start this final unit on Troubleshooting.

!

To view the corresponding video on the course website, you can scan the QR Code displayed here or directly log in to the course website http://lms.defindia.org

Video Duration: 0:52 Seconds

Setting up Wireless Networks – Part II

Outomes

In order to keep the network in good repair, it is important to have suitable maintenance measures in place. This unit covers steps for setting up suitable maintenance procedures.

Upon completion of this unit you will be able to:

- Describe what troubleshooting is.
- Use simple troubleshooting techniques.
- List common troubleshooting tools.

Terminology

Troubleshooting: Identifying what is going on when things “go wrong”.

OSI: Open Systems Interconnection is a reference model created by ISO (International Standards Organization). It is an abstract description for computer network (communication) protocol design.

OLSR: Optimized Link State Routing Protocol is an IP routing protocol optimized for mobile ad hoc networks, which can also be used on other wireless ad hoc networks.

WISP: Wireless Internet Service Provider (WISP) is an Internet service provider (ISP) that allows subscribers to connect to a server at designated hotspots (access points) using a wireless connection such as Wi-Fi.

Problems with a wireless network are often invisible and can require more skill and more time to diagnose and remedy. Interference, wind, and new physical obstructions can cause a long-running network to fail. The main challenge of troubleshooting any communication network is to identify what is going on when things “go wrong”.

Troubleshooting Model

Rather than rebooting everything that is attached to a power cord or blaming the weather conditions, the OSI model can be used 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 independently of each other. The Internet protocol design follows a similar structure to the OSI model.

Table 4: OSI Model

Layer	OSI
7	Application
6	Presentation
5	Session
4	Transport
3	Network
2	Data Link
1	Physical

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).

Simple Techniques for Troubleshooting

No troubleshooting methodology can completely cover all the problems you will encounter when working with wireless networks. But often, problems come down to one of a few common mistakes. Here are a few simple points to keep in mind that can get your troubleshooting effort working in the right direction.

Don't panic: If you are troubleshooting a system, it means that it was working at one time, probably very recently. Before jumping in and making changes, survey the scene and assess exactly what is not working. If you have historical logs or statistics to work from, all the better. If others were using the system before it started having problems, ask them to help you by having them tell you what was happening before it stopped working. Be thorough, but don't make it sound like you are accusing them of breaking it.

They may have important information that will help you fix things and you want them to be on your side. Be sure to collect information first, so you can make an informed decision before making changes.

Make a backup: This applies before you notice problems, as well as after. If you make a complicated software change to a system, having a backup means that you can quickly restore it to the previous settings and start again. When troubleshooting very complex problems, having a configuration that "sort-of" works can be much better than having a mess that does not work at all (and that you can't easily restore from memory).

Even in a broken configuration, make a backup copy of the parts of the system you will be changing before you try to make significant changes. If your changes result in an even worse state than when you first started working on it, you will at least have a known situation to go back to.

Check if it's plugged in: This step is often overlooked until many other avenues are explored. Plugs can be accidentally (or intentionally) unplugged very easily. Is the lead connected to a good power source? Is the other end connected to your device? Is the power light on? It may sound silly, but you will feel even sillier if you spend a lot of time checking out an antenna feed line only to realize that the AP was unplugged the entire time.

Check what the last change was: If you are the only person with access to the system, what is the last change you made? If others have access to it, what is the last change they made and when? When was the last time the system worked? Often, system changes have unintended consequences that may not be immediately noticed. Roll back that change and see what effect it has on the problem.

Look at date/time stamps on files: Every file on a modern computer system has a date and time associated with it showing when it was created or last changed. On a properly running system, most of the system files will have date/time stamps from months or even years ago. If the system or network was running fine until an hour or so ago, files, which have a timestamp within the past few minutes to an hour ago, could provide clues about what changed.

Determine what still works: This will help you "put a fence around the problem". While complex systems like a wireless network can be made up of many different components, it is likely that the problem is only with a very small number of them. If, for example, somebody in a lab complains they can't access the Internet, check to see if others in the same lab are experiencing the same problem. Is there connectivity in another lab or elsewhere in the building? If the problem is just with one user or within one room, you would want to concentrate your efforts on the equipment in just that one space. If the outage were more widespread, perhaps looking at the equipment where your outside connections come in is more appropriate.

Do no harm: If you don't fully understand how a system works, don't be afraid to call in an expert. If you are not sure if a particular change will damage another part of the system, then either find someone with more experience to help you or devise a way to test your change without doing damage.

Identifying Common Problems

The most common problem a wireless network user will experience is not being able to connect to the network, or to the Internet. There could be many causes for common problems with the network. Issues with the router hardware, an Ethernet cable, a power adapter, electricity or the Internet Gateway could be a part of the problem. The troubleshooting process is to work through options and rule out issues by seeing what is happening at each part of the network connection.

Start troubleshooting by asking these questions and stopping at the first section where the answer is "no". These questions pertain to four key areas:

Table 5: Indentifying common problems

1.	Power	Is the router powered on?
2.	Access Point Visibility	Can you see the access point on your client device?
3.	Association of Access Point with Client	Can you connect to the access point with your client device?
4.	Mesh Links	Are you not seeing the splash page after associating with the access point?

1. Is the router powered on?

It has the following scenarios:

a. Does the Power over Ethernet (PoE) adapter have power?
Make sure the PoE adapter is fully plugged-in to the electrical socket and that the power light on the PoE adapter is on.

b. Does the outlet work?

If the PoE does not turn on, check the electrical outlet with another electrical device that you know works. If that device also does not get power, try a different outlet.

If the power outlet works, the PoE adapter may be bad. Try replacing the PoE adapter.

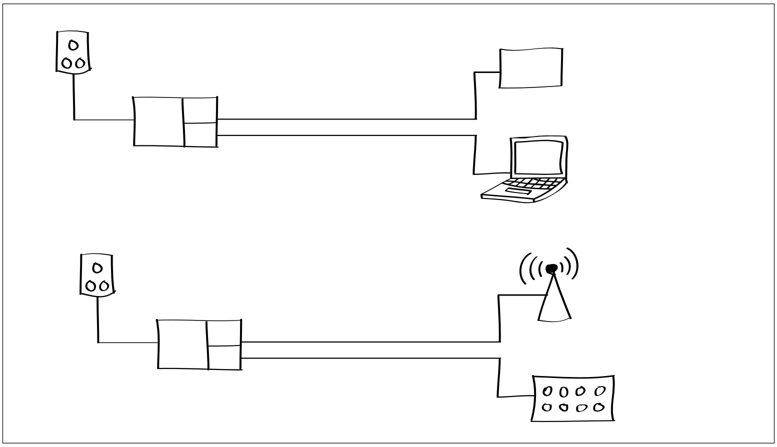


Figure 12: Example of showing power outlet

If the PoE adapter has power but the router does not, it may be a problem with the Ethernet cable between the PoE and the router. Try a different Ethernet cable.

Check to be sure all cables are securely plugged-in, between the PoE adapter and router, between the PoE adapter's LAN port and switch or Gateway modem (if applicable), and between the PoE adapter and electric outlet.

d. If the router still does not have power
If the above steps do not solve the power problem, unplug and re-plug the PoE adapter to restart the adapter and router. Wait a minute or two to let the router reboot before attempting to log in. If

this does not work, then there is a problem with the router and you should replace it.

2. Can you see the access point on your client device?

It has the following scenarios:

a. Are you near enough to the access point?
Make sure you are close enough to the AP for it to be visible to your wireless device. Also, check if any environmental conditions around the node are blocking the signal.

b. Is the access point hidden?
If you know there is an AP and you are close to the router, but you still cannot see the AP on your client device, the network administrator may have set the AP to invisible. Try entering the AP name manually on your client device in its network manager.

3. Can you connect to the access point with your client device?

Cannot connect to the Access Point: Your device isn't holding a connection.

a. Are you too far from the access point?
Because nodes often have more signal strength than your client device, you may be able to see a strong signal on your client device, but your client device may not be powerful enough to communicate with the node from a distance.

b. Restart wireless and/or your device
If you still cannot connect, try turning off and back on the Wi-Fi radio on your client device or restarting the device.

c. Make sure you are trying to connect to the AP, not to the ad-hoc (mesh) signal.
Usually, the difference between the two kinds of signals is indicated by their icon on your client device's network manager.

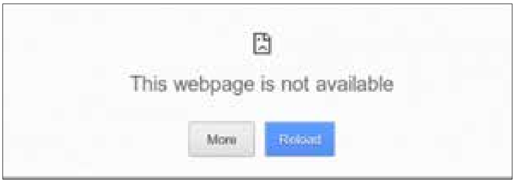
d. If the AP is secure, make sure you have the right network key, or password, for it
This is usually different from the root admin password.

e. Are there too many routers in the room?

There may be too much interference on the same Wi-Fi channel. To reduce interference, try removing some routers, spacing the routers further apart, or turning down the power on some of the routers.

4. Are you not seeing the splash page after associating with the access point?

No Welcome Page: If you are on the AP but aren't directed to the landing page (fig. 13)



This webpage is not available

Figure 13: Showing the example when AP is not connected

a. Check the status of the network

If you are associated with an AP and you know there is an upstream Internet Gateway in the mesh, but you cannot get online, there may be a broken mesh link. Make sure that all the nodes are meshing properly to the Gateway. You can check the node's host net announcements (HNAs) list to see if any nodes on the network are providing a gateway.

b. Check for a Gateway

Go to Advanced -> Status -> OLSR and then click on the HNA tab. This lists any non-mesh subnets attached to the mesh network, such as client networks and gateways to the internet. If the node has an announced network entry of 0.0.0.0 anywhere in this list, then it knows there is a Gateway to the Internet somewhere in the network. If the node does not have a 0.0.0.0 entry in the list, then it does not see a route to the Internet. Check the mesh network connections to make sure that all routers are meshing properly, and that the signal links are strong enough between nodes.

Troubleshooting Tools

Classifying technical problems is not an easy task as the problems vary from network to network. A simplistic way of looking at technical problems is to classify them as:

» Things do not work at all – For example, 'why doesn't my computer start?'
» Things work sometimes – For example, '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 monitoring all the wireless parameters during a period of time while trying to identify the cause of the problem.Displayed below is a set of tools that can help troubleshoot at each layer:

Table 6: Set of tools to help in troubleshooting

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		

Troubleshooting Scenarios

Scenario 1

Customer: "I cannot read my Hotmail!"

Table 7: Troubleshooting steps

Troubleshooting question	Reasons
What program do you use to check your e-mail?	Checking for application problems
Can we check the proxy settings of your program?	
Are you able to access other websites?	Checking for DNS problems
Does your application time out?	Checking for session TCP problems
Have you been able to login to Hotmail?	Checking for Authentication Problems
Is the Hotmail website loading?	Checking for routing problems
Can you tell me your IP address?	Checking for IP problems

Scenario 2

Customer: “My Internet is very slow!”

There is no simple and cheap way to monitor all the parameters involved in the “physical layers” of your wireless network. When troubleshooting the “radio” we use tools that talk with the “wireless cards” and retrieve a limited set of information.

By using a program like “Netstumbler”, a wireless card acts as a simple “spectrum” analyser that can scan for existing networks, their signal to noise ratio, modulation technique and operation mode.

Netstumbler is a “passive” software that eavesdrops wireless traffic from the network. Not all the wireless cards allow monitoring wireless traffic promiscuously. Before installing Netstumbler, check that your wireless card is supported.

Summary

UNIT SUMMARY

In this unit, you learned about basic troubleshooting techniques. You learned about the OSI model that can be used to identify the cause of the problem. You also learned about some common tools that can be used for troubleshooting problems that may occur due to power, access visibility, and association of access point with the client or related to mesh links.

Appendix

REGULATORY ENVIRONMENT FOR COMMUNITY NETWORKS IN INDIA

The Government of India has come up with one license for all telecom related services, known as Unified License under its Telecom Policy 2012. One of the objectives of the National Telecom Policy-2012 is "Strive to create One Nation - One License" across services and service areas. Under the Unified License, there are three kinds of licensing authorization processes to become Internet Service Provider (ISP), depending upon scale or the City/State /Town/District/ Village that anyone wants to start the ISP business in. The 3 categories are differentiated by the scale of the territory/coverage area of the ISP license i.e. whether the License is for (i) national area, (ii) major states/metro cities or (iii) other smaller cities, towns, villages and districts.

1. Class A (National Area) – This license is for Pan India operations.
2. Class B (Telecom Circle/Metro Area) – Class B license is issued for a total of 20 major states or any of the following Metro Cities – Mumbai, New Delhi, Kolkata, Chennai.

   The government keeps issuing notifications regarding territories declared as telecom circles and metro areas from time to time.
3. Class C (Secondary Switching Area) – This license is for only a particular secondary switching area. A secondary switching area is a government-defined territory, which could comprise of several small villages, towns or even districts. A class C license holder will have access to any 1 particular SSA only unless he applies for multiple authorizations under one unified License.

To become an ISP, one must acquire a Unified License under which he will obtain Authorization for providing ISP services. Hence, it must be understood that there is no "ISP License" as such. Instead, one must obtain ISP Authorization under the Unified License. One company can hold only one Unified License but can apply for authorization of multiple services and/or service areas.

The following table will explain the financial entry conditions you require to fulfil in order to obtain a Class A/B/C ISP license:

Table 1: Financial entry conditions to obtain ISP license

Service	Minimum Equity	Minimum Net worth	Entry Fee (Rs.)	Performance BG (Rs.)	Financial BG (Rs.)	Application Processing Fee (Rs.)	Total Capital Required (Rs.)
ISP "A" (National Area)	Nil	Nil	15 Lakh	Nil	50,000	50,000	16,00,000
ISP "B" (Telecom circle/ Metro Area)	Nil	Nil	1 Lakh				
	Nil	50,000	15000	1,65,000			
ISP "C" (district)	Nil	Nil	10,000	Nil	5000	10000	25,000

There is another kind of license process, known as Virtual Network Operator (VNO) or mobile virtual network operator (MVNO), which is a provider of managed services and a reseller of network services from other telecommunications suppliers that do not own the telecommunication infrastructure. These network providers are categorized as virtual because they provide network services to customers without owning the underlying network. A VNO typically leases bandwidth at the wholesale rates from various telecom providers in order to provide solutions to their customers. The difference between ISP and VNO is given below the table 2:

Table 2: Difference between ISP & VNO license

VNO License	ISP License
Issued for a duration of 10 years.	Issued for a duration of 20 years.
The license terms can be reviewed in every 4 years by DoT.	Once issued, the license will be valid for 20 years no matter the changes in DoT policies.
Lesser bank guarantees to be submitted.	More bank guarantees are to be submitted.
You cannot provide ISP franchise to local service providers	You can provide ISP franchise to other operators in your area of jurisdiction.
Lesser Hardware implications.	More hardware implications.

Fully virtual VNOs do not have any technical facilities or technical support provision instead they rely upon the support delivered by the owners of the underlying infrastructure. The VNO concept has gained a lot of traction in the telecommunications industry, as the cost of infrastructure is substantial.

But even if any company is not able to apply for ISP or VNO license, then any small-level entrepreneur can buy the bulk bandwidth from the main ISP and resell it and become a franchise.

IP ADDRESS CLASSES

There are five classes of available IP ranges: Class A, Class B, Class C, Class D and Class E, while only A, B, and C are commonly used. Each class allows for a range of valid IP addresses, shown in the following table 3.

Table 3: ISP and their range of IP addresses

Class	Address range	Supports
Class A	1.0.0.1 to 126.255.255.254	Supports 16 million hosts on each of 127 networks.
Class B	128.1.0.1 to 191.255.255.254	Supports 65,000 hosts on each of 16,000 networks.
Class C	192.0.1.1 to 223.255.254.254	Supports 254 hosts on each of 2 million networks.
Class D	224.0.0.0 to 239.255.255.255	Reserved for multicast groups.
Class E	240.0.0.0 to 254.255.255.254	Reserved for future use, or research and development purposes.

Setting up Wireless Networks – A Course for Barefoot Wireless Engineers has been produced by the Digital Empowerment Foundation. This course is divided into two parts. The first part covers some basic concepts related to planning the setup of wireless networks such as conducting a location survey and selecting the required hardware. The second part of the handbook covers details of actual installation and maintenance of wireless networks.

C·O·L COMMONWEALTH of LEARNING
Learning for Sustainable Development

DEF
DIGITAL EMPOWERMENT *foundation*