Start and Build a Successful Wireless Internet Service Provider (WISP) Business

A guide for the WISP entrepreneur with a limited budget, limited time and limited technical knowledge

John D. Barker, Ph.D., MIEEE

Start and Build a Successful Wireless Internet Service Provider (WISP) Business:

A guide for the WISP entrepreneur with a limited budget, limited time and limited technical knowledge

For publication in 2022

Contact the author at: john@fire4.com

Please contact the author for a Spanish version of this book.

Contents

Preface

While the rate of expansion of the Internet has been rapid there is sill a sizable part of the global population that does not have access to the Internet. There are two reasons; the first is that the infrastructure to deliver the Internet to some people has not been built, and second, infrastructure is available but the cost is outside the economic ability of the people wishing to have Internet access. There are several types of service providers that deliver an Internet connection to customers.

- Government telecom entities with no competition, these entities make few investments with infrastructure; access to basic telephone services is limited.
- Large private telecom entities usually have few competitors because they buy the competitors to maintain high prices. Areas of coverage are limited to those that give the best return on investments so that they can generate good profits and pay dividends to shareholders. Rural areas get poor or no telecom access.
- Satellite Internet providers, there are few companies providing this service because the cost of investment is very high, and most companies have become bankrupt because they cannot achieve break-even and provide a return on the initial investment. Satellites in geo-stationary orbits have limited bandwidth, high latency and high cost. Low earth orbit (LEO) satellite businesses have failed, however the SpaceX Starlink service will likely succeed because the number of satellites proposed (30K+) will provide the global coverage required.
- Small Internet service providers that purchase wholesale Internet access from large telecom entities and then build out a network to resell the service to individual customers. The ‘last-mile’ service is usually delivered as a wireless link because it is the lowest cost method, and so these businesses are called Wireless Internet Service Providers (WISP’s). The WISP cannot extend the network range beyond approximately 50Km from the point of access to the wholesale circuit.
- Individuals or very small service providers who are paying for a retail Internet connection and then reselling to others, sometimes without the knowledge of the Internet vendor. This is a popular method in developing economies where the economic ability of individuals is limited.

Even in countries with a high level of technology a proportion of rural customers cannot get Internet access because the large telecom businesses consider the cost of providing rural Internet uneconomic for them to do so. This leaves an opening for smaller WISP businesses that have a lower cost structure then the telecom companies to provide an Internet service for the rural customers.

A significant percentage of people in countries with developing economies have no access to the Internet because there is no infrastructure. Even in urban areas where an Internet service is available the cost is higher than many people can afford. In areas of the world such as Latin America, the Caribbean and Africa WISP's are the driving force for the expansion of the Internet outside the urban areas. The USA and Europe still have rural areas without Internet access and small private WISP businesses have established operations as Internet providers for some under-served rural areas. Rural areas in the USA that have no service can contract geo-stationary satellite access.

LEO satellite services are being deployed and promise to connect the people without Internet services, however to cost is higher than geo-stationary satellite services. The cost of satellite services will exclude many rural residences in the USA, and is certainly out of reach for people in developing countries.

When the LEO satellite services finally have global coverage and their terms of service permits businesses to re-sell the access then it will be possible for a WISP in a remote location to install a Starlink antenna on a tower and provide Internet access for 10’s or a few hundred people, with a very low monthly cost for each customer.

Until now setting up and operating a WISP business requires a thorough technical understanding of computer networking technology. WISP’s that have been established in the USA and EU were in most cases started by individuals with many years of experience in IT with a strong background in networking including skills learnt with the help of Cisco certification courses. Countries with developing economies do not have a large pool of networking professionals; there are few IT businesses and the opportunities to learn computer-networking skills are not available.

The author has worked with the global Internet service provider industry for many years, designing products for ISP’s and WISP’s that are used to manage and deliver Internet services. The author has also trained many individuals and advised businesses about technologies that will enable them to improve performance, reliability and profits while reducing costs. The author’s customers are located in North America, Europe, Central and South America, the Caribbean, Asia and Africa.

Starting a WISP business is especially challenging for entrepreneurs; there is little access to investment capital and little access to the specialist technical knowledge required. Developing countries have further business challenges, payments, collections and government bureaucracy. WISP’s in developing countries are receiving cash payments for the Internet services as many customers don’t have bank accounts or credit cards.

The author has participated with the development of products that are geared towards developing markets; prioritizing low investment costs, low operating costs and simple configurations that are easy to use and do not require expert knowledge.

Individuals seek out the author with the frequently asked question; “how do I start a WISP”. The author has answered this question on many occasions, through the preparation of training documents, seminars and publications with the objective of helping people who have limited access to technical knowledge and little business experience to establish and build a successful WISP business.

This book was prepared to answer this question for a broader audience; people who have the ambition to start a WISP business, but are seeking both technical and business information, that will give them a direction to start and the guidance to build the business with a minimum investment cost.

In addition to working with WISP's in emerging economies, the author also has first hand experience of the benefits that Internet access can bring to poor and developing economies through service as a member of Rotary International with global grant projects. One example of these efforts is that women in rural Colombia have been able to start small coffee growing businesses because the Internet gives them access to the global marketplace to sell their produce.

The availability of wireless broadband Internet access is not only a business opportunity for a WISP, but also an opportunity for people with limited economic means to have access to the Internet and improve their lives through becoming part of the global economy; people who would otherwise be excluded from economic opportunities.

1. The business of selling Internet access

1.1. The Internet entrepreneur

One of the fastest growing service businesses worldwide is the connection of people to the Internet. Some countries are more advanced than others in terms of the percentage of the population who have access to the Internet. Populations in urban areas are better served with Internet services whereas populations in rural areas are underserved. The large telecom companies in each country have limited budgets to build out network infrastructure and so their priority is to spend on infrastructure in urban areas where they can connect the maximum number of paying customers to the Internet, and get the best return on investment. Communities in rural areas are therefore geographically excluded from access to the Internet. Large telecom companies around the world, especially the government monopolies, have high operating costs and so charge customers a high price for the Internet service. This means that part of the population is economically excluded from access to the Internet.

Large wire-line telecom providers connect Internet customers with copper or fiber cables that have a high installation cost and so the charge for their service is high. Wireless telecom providers made significant investments in the construction of 3G, 4G and now 5G wireless networks for mobile devices, which result in a high cost for the customer. The mobile service providers put data caps on the service that limit the customer's monthly data use. Mobile network coverage in rural areas is limited as few towers are constructed where the population density is low.

In many countries entrepreneurs address the two issues of geographic and economic exclusion of parts of the population from the Internet. The entrepreneur can provide a low cost service in rural areas by building a network that connects to a wholesale service that is contracted by the entrepreneur.

The entrepreneur can provide the Internet service for a lower cost than a big telecom provider for two reasons. First, the cost of building a wireless network is much less than the cost of building a wired network or mobile phone network. The second reason is that the operating costs of the small entrepreneur are much less than those of a big telecom business. The business that the entrepreneur builds to deliver the Internet service to parts of the population is called a Wireless Internet Service Provider (WISP). This book explains what the entrepreneur needs to know to start, operate and grow a profitable WISP business, and to address the demand from people who want Internet access but otherwise have no other means to connect to the Internet. The Internet is extremely important for people in countries with developing economies, as it is a path for those people to become part of the global economic community.

1.2. The markets for Internet services

There are several broadband methods of delivering Internet access to customers, listed below.

- Wired broadband via cable using a DSL, cable TV service or fiber connection provided by an Internet Service provider (ISP).
- Wireless broadband via 3G/4G wireless to a smart-phone, provided by a mobile phone company.
- Wireless broadband via WiFi wireless to any type of fixed wireless or mobile device, provided by a Wireless Internet Service Provider (WISP).
- Wireless broadband via satellite, which can be geo-stationary (e.g. Hughes) or low-earth-orbit (e.g. Starlink) to a ground receiver.

There are two classifications for wireless broadband customers.

- Fixed broadband, Internet access is delivered to a home or business using permanent wireless connection, which then provides a wired and a wireless connection inside the building to connect devices.
- Mobile broadband, Internet access is delivered to a mobile device, smart-phone or tablet, using a 3G/4G wireless service (mobile phone operator) or a WiFi wireless service (Wireless Internet Service Provider).

The demand for Internet access services is growing quickly for many reasons.

- Communicate through the Internet using Apps like Skype and Zoom instead of making phone calls.
- Use social media.
- Switch to buying on-line instead of going to stores.
- Use the Internet to manage money and pay bills due to limited access to banks.
- Using the Internet to search for information.
- Access to educational courses through the Internet.
- Work from home using Internet access.

The demand drives businesses to invest in providing Internet services.

- Businesses provide Internet access to attract customers: motels, hotels, restaurants, cafes, shopping malls, retail stores, etc.
- Public services provide Internet access for visitors: schools, hospitals, municipal offices, etc.
- 3G/4G coverage is poor in rural areas and overloaded in urban areas so alternative Internet services are popular with mobile phone users.

- Telecom companies charge high prices and impose data caps for 3G/4G Internet data services so alternative lower cost services are popular with mobile phone users.

Selling Internet access is a great opportunity for any entrepreneur who wants to build a business with very little investment using low cost WiFi equipment. WiFi is the lowest cost technology for Internet access. All computer and mobile devices can connect to WiFi.

1.3. WISP and ISP services

Many people get broadband Internet service from an Internet Service Provider (ISP) via a wired connection. The ISP is a phone service providing an ADSL (asymmetric digital subscriber line) service, or a cable TV Company providing a cable modem. The ISP provides the connection for the Internet data service and the data connection is used to deliver other services that include telephone and TV. Streaming TV is a very popular service that is replacing satellite TV dishes for customers with an Internet connection. Other services that an ISP might provide include home security and services for business such as web hosting and off-site data backup. The most popular form of data connection is ADSL over twisted pair copper wire and cable connection over coaxial wire but optical fiber is becoming more common in urban areas. Optical fiber has a big advantage over copper wire that the data speed can be much higher. Optical fiber has symmetrical data rates, the uplink speed is the same as the downlink speed, and ADSL is asymmetric meaning the uplink speed is much slower than the downlink speed.

The Wireless Internet Service Provider (WISP) provides a wireless connection to the customer’s premises or mobile device. The principal WISP service is the Internet connection however the WISP can offer additional services such as a telephone service using a voice-over-IP (VoIP) protocol and streaming TV. The wireless connection is generally not as reliable as a wired connection as atmospheric conditions and vegetation in the path of the wireless connection can reduce the connection quality. The benefits of the wireless connection are that the installation cost is much lower than a wired connection and data speeds can exceed those of an ADSL service. In some rural locations the mobile phone service is not available due to the low density of towers and there is no ISP service. The customer has the options of a satellite Internet service or a WISP service if available. The WISP has a contractual agreement with the wholesale telecom company for a very fast connection to the Internet then distributes and sells the service to the WISP’s customers.

Wireless Internet service customers are classified into two groups of fixed and mobile wireless broadband services where each requires a different technical method of providing the Internet service.

Most WISPs’ in the USA and Europe offer a fixed broadband service. The fixed broadband customer has an obligation to pay for the service every month. Fixed wireless broadband requires an installation of wireless and network equipment in the customer’s premises. This installation has a cost and the customer either pays this at the time of the installation or else a fraction of the cost is added to each monthly payment when the customer agrees to a fixed term contract.

Mobile broadband WiFi services are provided on-demand and accessed by mobile devices. The on-demand mobile service cost for the customer is much less than the fixed broadband service so is popular with those parts of the population that have economic limitations. WISP’s in developing economies offer both fixed and mobile broadband because many people in emerging economies want access to the Internet but cannot afford the installation cost and monthly payments of fixed broadband. Mobile broadband provides a low-cost alternative for customers. The mobile broadband is provided at specific locations and the customer has to go to a location where the service is available. The customer will purchase a voucher for Internet access that has a time or duration limit. This is called on-demand billing because the customer purchases limited Internet access when the customer needs the access. A WISP that is growing in an emerging economy will find that there are many more customers for mobile wireless broadband than there are for fixed wireless broadband due to the economic constraints of the population. The availability of mobile wireless broadband is not only a business opportunity for a WISP, but also an opportunity for people with limited economic means to have access to the Internet. The mobile broadband service is often a cash sale in emerging economies, as many customers do not have bank accounts or credit cards.

1.4. WISP fixed wireless broadband services

Fixed wireless broadband provides a wireless Internet connection to the customer’s premises that will be a residence or a business. The service provider will install a directional antenna on the roof of the customer's premises for long-range data communications with the wireless point-to-multi-point (PtMP) antenna installed on a distant tower. The fixed broadband customers location may be several Km from the PtMP antenna that provides the Internet connection. The customer has continuous access to the Internet. Within the customers premises there is a local area network (LAN) with both wired and WiFi wireless connections. The LAN network will connect different types of devices that include desktop PC’s, laptops, gaming products, tablets and mobile phones in WiFi mode.

The fixed broadband customer provides billing information for the service provider and will pay a fixed monthly fee for the broadband service. The customer pays the fee either before the start of each month of service (called pre-pay) or else pays after the month of service has been completed (called post-pay). If the bill is not paid then the service is temporarily interrupted until the bill is paid. The WISP may also provide the fixed broadband customers a pay-on-demand service as an alternative to having a fixed monthly payment.

The service characteristics that a WISP will provide for fixed broadband customers are as follows.

- The broadband service is to a fixed location, home or business, via a point-to-point wireless connection, range is up to several Km from the wireless access point but must be line-of-sight. The service provider is responsible for the installation of a wireless antenna (customer premise equipment: CPE) on the customers building roof for long-range communication (several Km) and also to provide a network connection inside the building, usually by installing a wireless router.

- Each fixed broadband customer will agree to a payment method so that the service can be billed monthly. The service provider can offer alternative payment methods for the customer that include, check, credit card, and cash.
- The WISP may permit a fixed broadband customer to purchase Internet access on demand if the customer prefers; a similar payment scheme to that of the mobile broadband customer.
- The customer is authenticated onto the broadband service network by providing a credential; the credential will be pre-programmed into the client wireless equipment by the WISP.
- The customer's broadband service is always connected to the Internet, unless payment is not made in which case the service is interrupted.
- A customer relationship management (CRM) portal provided by the WISP permits the customer to pay bills, see invoices and check Internet use.

1.5. WISP mobile wireless broadband services

Mobile broadband is a wireless service that is provided for mobile devices, such as smart-phones and tablets that use WiFi technology. The mobile broadband customer is anonymous and will purchase a credential, usually an access code, to get Internet access. The mobile wireless broadband customer has access to the Internet for a pre-determined duration after a credential has been first used. Mobile broadband is called an on-demand Internet service because the service is used for a limited period of time when the customer requires it. Some WISP's offer a monthly subscription plan for mobile broadband customers who use the service frequently.

Most people are familiar with an on-demand mobile broadband service. The service is sold in airports and used by travelers who do not have roaming access to the local mobile phone service and require Internet access. The service is also sold at locations where there is no mobile phone service such as campgrounds and RV parks. Some hotels provide a 2-tier Internet service where a slow Internet speed is provided for free, however the guest must purchase the fast Internet service if required.

Mobile broadband technology is different in operation to the WiFi that is installed in a home or office building. Mobile broadband supports customer roaming, which is managed by a cloud-based service. When the customer connects to one WiFi wireless access point using a credential the customer will remain connected at all other WiFi points that are part of the same network even when the WiFi points are in different locations. The customer will only loose the connection when the duration of the credential expires. The mobile device communication range is limited to a few hundred meters to the PtMP wireless antenna due to the low power of the mobile device WiFi.

The service characteristics of mobile broadband are as follows.

- Each mobile broadband customer is anonymous; there is no agreement for payment that requires the service provider to have knowledge of the customer; the customer purchases a credential or access code to get Internet access.
- Mobile broadband customers will pre-pay for the pay-on-demand Internet service when they wish to use it, which means purchasing an Internet service credential. The service is measured either by duration (e.g. 1-day, 1-week, 1-month) or by data limit (e.g. 1GB download, with 100MB upload limit).
- Each mobile broadband customer may have several devices that have WiFi wireless technology (smart-phone, tablet or laptop), and can use any device with the mobile broadband service.
- Each mobile broadband customer can connect to any designated wireless access point within the range of the mobile device and connect to the Internet using an access code via a login page.
- It is advantageous for the WISP to provide the mobile broadband service available at as many locations as possible.
- Mobile broadband customers require roaming so that they can move between many wireless access points and get Internet access when required.
- The majority of mobile broadband users in the USA and Europe are travelers who wish to maintain Internet contact while traveling, but mobile phone communication is not available to them.
- The majority of mobile broadband user in emerging economies are people with limited economic means who need Internet access for the lowest possible cost.
- A limitation of mobile broadband technology is that the PtMP wireless access point is not encrypted and therefore can be hacked. A WISP can take measures to deter hackers.

The mobile broadband service providers network is built according to the types of customers to whom service will be delivered, which is determined by the location of the WISP.

1.6. Identifying and qualifying a WISP business opportunity

The entrepreneur has to gather some essential information about the prospective business opportunity in order to consider starting a WISP business.

- Is there a demand from a number of people who want the Internet service?
- What will be the cost and charge per customer for the Internet service?
- Can the prospective customers afford the service?
- What is the minimum number of customers that will ensure the business is not operating at a loss? This is called the ‘break-even’ number.

- Is any other provider offering an Internet service and will be a competitor?
- Does the entrepreneur have access to a wholesale Internet provider with a reliable service?
- Does the entrepreneur have the technical and managerial skills to establish and build a WISP business?

A later section will explain the requirements for starting and growing a WISP business and will provide answers to these questions.

1.7. Branding the broadband Internet service

When starting a business to provide wireless Internet access for mobile customers it is very important to create a clear and easily recognized brand. Once created the brand can be developed as a trustworthy vendor who provides a high quality and reliable service. Developing the brand is important for two areas.

- Sales, marketing with name recognition.
- Growth, trust and reliability.

With an established brand, enthusiastic customers can become part of the sales organization to bring referrals, which will drive business growth. The results of good branding are that the broadband Internet service will not only increase sales month by month but the business equity will increase in value. There are various points of contact with the broadband service that require branding. Some of these are listed below.

- Business website.
- On-line contact with the business services, e.g. CRM portal, technical support.
- Advertising material.
- Written communications with customers.
- Professional interface during telephone contact with the company.
- Premises installation, technicians with good appearance, professional attitude, identification badge, uniforms, branded equipment, truck or van with logo.
- Branded bills and receipts issued to customers.
- Brand training for customer facing staff.

Wireless Internet service providers that offer mobile broadband also have two additional items that require branding.

- Wireless login page (Hotspot).
- Access code vouchers.

It is worthwhile to pay a public image or marketing firm that can develop the branding for the broadband Internet Company.

1.8. Internet Service Sales and Marketing Techniques

The most important task for a broadband service provider is attracting new customers. Marketing describes a set of tasks that create an awareness of the Internet service with potential customers and should attract them to purchase the offer. Marketing can be accomplished using methods and some typical methods are listed below.

- Door to door distribution of flyers within the antenna coverage area.
- Advertising through popular mediums; local newspapers, etc.
- Advertising posters and flyers in locations of high foot traffic; supermarkets, shopping malls, etc.

The methods chosen depend on the situation where the service will be installed. The content of the advertising material can include.

- Explain the unique advantages of the service.
- Irresistible offers, first month free if purchased within 5 days, etc.
- Lower cost or better service than a competitor.

Potential Internet service customers must be in range of the antenna or antennas. Anyone outside the range of the antennas will not have access to the Internet service.

Probably the most effective marketing method is the door-to-door distribution of flyers within the service area of the antenna, with the flyer advertising a unique or irresistible offer. The business will have a website with additional information that can be accessed by anyone seeking further information, and should have a method to collect contact information from people who want to ask questions about the service.

The purpose of marketing is to generate leads. Leads are calls or messages that are received, or messages sent via the website, from people who are responding to the flyer.

The sales process follows on from the marketing process, and its purpose is to convert sales leads into paying customers. The sales process depends on the location and the types of potential customers.

The WISP can install a retail store where people who are attracted by the marketing can go to speak with a knowledgeable person and eventually purchase the service. The sales person will seek to commit a customer to a monthly subscription.

A retail store is important when payments are received in cash. In some countries cash payment gateway services are available, such as Oxxopay in Mexico. If prospective customers can make payments with credit or debt cards then sales can be made on-line with telephone support.

There are four principal marketing strategies to develop sales of the Internet providers business, listed below.

- Advertising flyers: Tell the potential customers about the Internet service by printing flyers and posting them through letterboxes within the antenna coverage area. Flyers can also be distributed via retail businesses.

- Customer loyalty program: Offer benefits to broadband Internet customers who add additional services to the broadband agreement.
- Referral reward program: Have customers work as salespeople, offer rewards for referrals of new customers.
- Subscription program: Guarantee monthly cash flow by attracting subscribers using attractive offers that lower the cost for a customer who assumes a long term commitment.

1.9. Mobile broadband subscription services

A number of Internet service provider businesses have been established to provide mobile Internet on a national or global scale. All have cloud-managed services that issue access credentials to subscribers. All of these systems implement mobility but none of them implement roaming. Subscribers create an account in the same way that they would for a fixed broadband provider and pay a monthly subscription. The subscription permits the customer to access the branded wireless mobile broadband access points anywhere in the world. The mobile broadband subscription systems are very popular with travelers who wish to connect to the Internet at International airports. The names of some well-known mobile broadband wireless Internet providers are shown in the figure. The best known of these mobile broadband businesses is Boingo who provides wireless broadband Internet at many airports throughout the world.

Figure 1.9.1. Well-known brands that provide a wireless mobile broadband Internet subscription service.

1.10. Network infrastructure

The WISP delivers the Internet service to the customer by building a network infrastructure. The network infrastructure connects the customer to the wholesale

Internet connection and is built using wired and wireless network components. A later section of this book describes the technology of the network components and design of the network infrastructure.

Designing and building the network infrastructure requires knowledge of computer networking, including configuring wireless equipment for point-to-point wireless links and point-to-multipoint wireless installations. The entrepreneur must have basic networking skills before considering the development of a WISP business, or else bring a technical partner with these skills into the business.

There are two important aspects of the network infrastructure design and installation, reliability and cost. The network must be reliable, as subscribers who don’t get a reliable service will leave quickly. Cost is also an important factor as a high initial infrastructure investment will increase the customer charge and this may make the project unviable. There is a trade off between infrastructure cost and reliability.

Network infrastructure performance is also important for customers who will complain if the network is slow. In order to maintain good performance of the network infrastructure the WISP requires a means of monitoring the network for performance bottlenecks and to be alerted when a failure with any component or segment of the network occurs. Network circuit segments each have a maximum bandwidth, which is the maximum number of bits per second that can flow through that segment. It is important for the WISP to know when a segment has reached maximum capacity, as the service to the subscriber will be degraded if the demand on capacity exceeds the maximum. The WISP has the option to increase the network segment capacity, or route the subscriber through a network segment that has available bandwidth. The network monitoring software should also maintain an inventory of all components in the network. The WISP requires a procedure in place for the field service technician to make changes to improve network performance and repair any component failures quickly.

1.11. Structure of the WISP business

All businesses have a well-defined structure and organization that permits the business to function. For example, a retailer requires a store location with utility services, sales staff, buyers, stock manager, and financial accountant. Similarly a WISP business has a structure and organization that must be assembled in order to build a viable business. The basic function of a WISP business is to build and operate the communications infrastructure that will connect many customers to one wholesale Internet circuit. This is shown in the next figure. The network infrastructure is divided into two parts. The first part is the infrastructure that connects from the WISP office to the wholesale Internet provider, which may be copper cables, optical fiber cables or a point-to-point wireless link. The second part is the network infrastructure that connects many customers to the WISP office; this part of the infrastructure is called the wireless distribution network. Connecting the two network infrastructures is a component called the access control. This component is necessary to allow the customers to connect to the Internet only when they have paid for the service, and it also applies the rules of the service, such as the maximum data speeds.

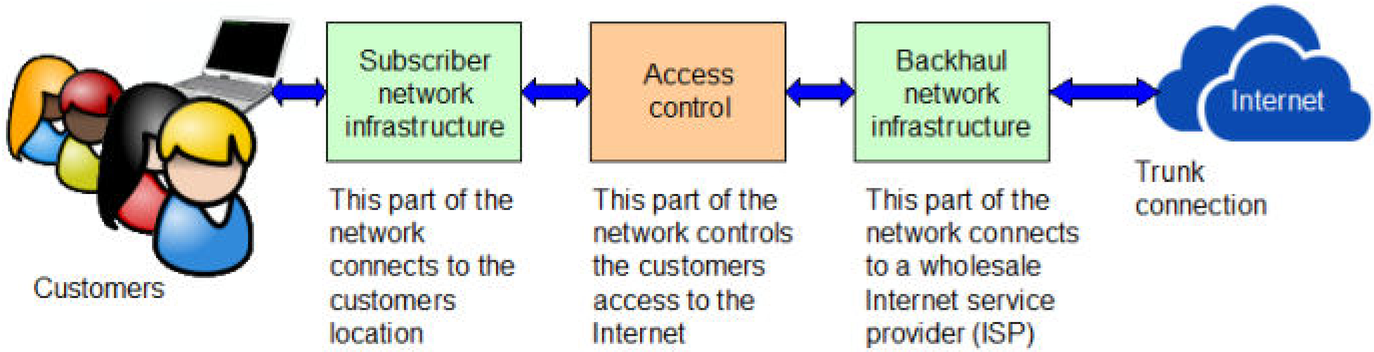


Figure 1.11.1. Basic function of the WISP business.

Building the infrastructure is not enough to operate the WISP business; other functions are also required to operate the business. The first of these is billing. The billing process can be as simple as a spreadsheet where the WISP owner checks each day to see which customers have to be charged for the service. This method is appropriate when the WISP is starting in business but it does not scale well and is burdensome when trying to manage hundreds of customers. If the customer does not pay a bill then the WISP owner has to disable the access control for that customer manually. There are accounting packages such as Quickbooks which can semi-automate the billing process by programming reminders when invoices have to be printed and sent out. The WISP owner still has to check that the payment has been received and disconnect the customer manually if not paid. The next level is billing software that is designed specifically for WISP's. This software provides more billing features than the generic accounting software, however the customers still have to be disconnected manually if the bill is not paid. The final level is billing software that sends instructions to the access controller. The software programs the service characteristics into the access controller, such as data speed, for a new customer. The billing software also disables the customer automatically if the bill is not paid on time. This level of software also eliminates the need for the WISP owner to have a deep technical understanding of programming the network router used for access control. To summarize, the four levels of billing implementation are as follows;

- Spreadsheet to track customer payments.
- Accounting software with accounts receivable and invoicing.
- WISP billing software that requires manual access control programming.
- WISP billing software that automates the access control programming.

The following diagram illustrates how the billing software integrates with the WISP infrastructure; there are two inputs and two outputs for the billing module.

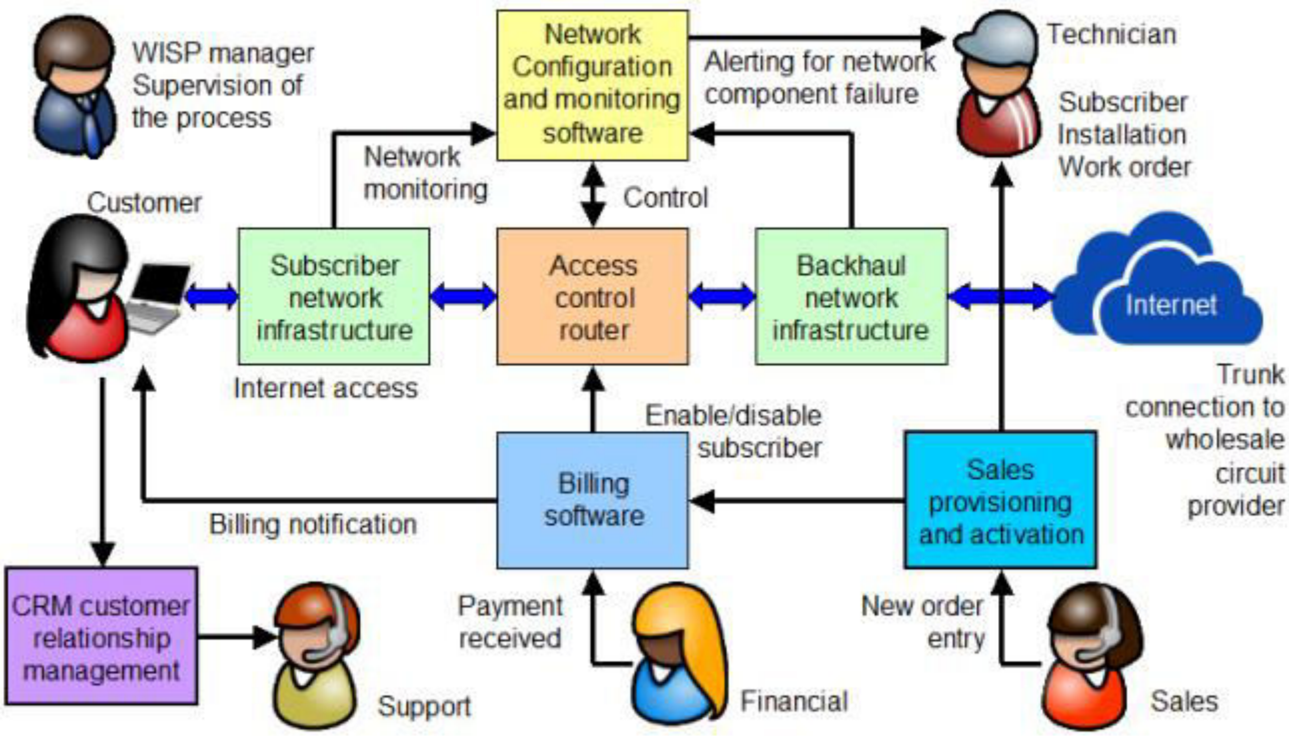


Figure 1.11.2. The WISP business management processes.

The first input is the entry of new customers to the billing system; the customer billing information is provided plus the start date of the monthly billing cycle, and the parameters of the service that include the maximum download and upload speeds, called the customer rate plan. The second input is from the payment processor to advise that the payment has been received. If the payment is not received by the due date then the customer is temporarily disconnected from the Internet.

The first of the two outputs is the billing notification, the invoice, which is printed and posted to the customer or sent electronically to advise the customer that the payment is due. The second output is the information to program the access control. This can be information that the WISP owner will access and then program the access control manually, or else the billing system interfaces directly to the access controller to program the unit automatically. The latter is the preferred case for the non-technical WISP.

Additional modules required to manage the WISP business are described in the following paragraphs.

The sales, provisioning and activation module might be part of a WISP billing software. The function of this module is to permit the addition of new customers then perform two tasks for the new customer. The first task is the creation of a work order for the installation technician who will go to the customer's premises and install the wireless and network equipment that will provide the customer with Internet access. The second task is to add the new customer to the billing system and advise that the customer should be activated for billing as soon as the customer is connected to the Internet. This will require an input from the field service technician that the installation is complete and functional.

The next module is the network monitoring and failure alert. This may require two software packages. The manufacturers of the wireless equipment will provide software for configuration of the wireless products; which could be remote access software or cloud management software. This software is essential for the WISP and will avoid trips to remote sites to program the equipment. The second part of this module provides the ability to monitor all network equipment and identify and alert the WISP owner when a failure occurs. Without failure monitoring the WISP only knows about a failure when an angry customer calls, which is not good for customer relations. It is also desirable to test the network connection out to the customer's location, as customers will call to say that they have no Internet and so the test is necessary to determine if the problem is in the network or at the customer's premises.

The final module is customer relationship management (CRM). This module is a portal or website interface that provides information and technical support for the customer. The quality of customer service is very important as poor service will lead to the customer becoming frustrated and canceling the service. The basic minimum requirement for customer support is a telephone number where the customer can call to ask questions and get issues solved. A better level of support is provided with a branded portal (a website login) which permits the customer to see the status of the account, print past invoices and open a support ticket which is a written request to the support staff. The support ticket is a very important tool for the WISP owner who wants to scale the business and maintain good customer relations. The owner can access the support ticket report and check for outstanding issues that have not been solved, then follow up with support staff.

The implementation of the management structure requires four job functions that are technician, sales, financial and support. The start-up WISP owner will probably be responsible for all functions initially.

Some roles are time and labor intensive, such as the field service technician and the sales staff. Such roles will eventually require multiple staff members to ensure that new customers are acquired and installed in a timely manner. When the WISP business grows sufficiently for the WISP owner to hire people for these roles then the owner can assume managerial and supervision roles to ensure that the processes run smoothly and the manager can correct any problems quickly.

There will be a constant addition of new customers as the WISP business grows, which will require constant expansion of the network infrastructure. The WISP owner will also have to seek periodic expansion of the wholesale Internet service for greater capacity with higher throughput to service the additional customers.

1.12. Billing customers

There are several methods to bill customers and several levels of services that can be provided for each method. The WISP owner must learn how to calculate the value that customers should be charged based on operating and investments costs. A method of calculation is described in the later section about starting and growing a WISP business. The value charged is for the monthly billing period and the payment date is on the same date of each month.

There are three methods of billing customers and the WISP can choose to implement one or more of the methods listed below.

- Pre-pay; the customer pays in advance of the billing period start date and if the payment is not received by this date the service is interrupted. The customer is requested to sign an agreement to use the service for a minimum period of time, usually 1 year. Many WISPS prefer pre-pay billing as it brings receipts forward by two months, which improves the cash flow of the business.
- Post-pay; the customer pays after the end of the billing period and is given a period in which to pay, usually within one month after the end of the billing period. If the payment is not received by this date the service is interrupted. The customer is requested to sign an agreement to use the service for a minimum period of time, usually 1 year.
- On-demand; the customer pays for a period of service when the customer requires it. This may be 1 day, 1 week or 1 month of service. The customer has no obligation to pay periodically as pre-pay and post-pay customers do. This method of billing is popular for mobile broadband applications.

The first two methods of billing are called monthly subscriptions so we call the customer a subscriber.

In addition to the billing method the WISP must decide about levels of service, called rate plans. A rate plan is the specification of the charge and conditions of the service, where the conditions include the maximum download and upload speeds, and possibly a monthly data cap. A WISP will have different types of customers, from residents of an economically limited neighborhood to wealthy businesses in an industrial area. The residents might prioritize low Internet cost while the businesses prioritize high speed Internet. The WISP will therefore develop several rate plans that suit every type of customer. A few example rate plans are shown below for an asynchronous data service, the value charged depends on the operating cost calculation.

- Maximum 5Mb/s download speed, 1 Mb/s upload speed: $15 per month.
- Maximum 10Mb/s download speed, 2 Mb/s upload speed: $25 per month.
- Maximum 20Mb/s download speed, 4 Mb/s upload speed: $40 per month.
- Maximum 40Mb/s download speed, 8 Mb/s upload speed: $70 per month.

The speed and price differential is made because the major operating cost of the WISP is the wholesale Internet service which has a cost and a maximum data rate so the cost per bit can be calculated when operating at maximum capacity. When the WISP has few customers then the operating cost per customer is high, so customers with a slow data rate are charged a higher price. The WISP can reduce the cost per bit for customers who have higher data rates.

1.13. Additional services

A WISP can offer additional services with the Internet access service to increase the income and profit per subscriber. Such services include telephone (VoIP) streaming TV and security surveillance with IP cameras. The WISP can contract with third party businesses that provide the services and there will be some investment to brand the services. Adding additional services is a good investment for the WISP who has built a network with the facility to increase data capacity and has a profitable subscriber base that can consume additional services.

1.14. WISP business regulations

Each country has rules and regulations that determine how a WISP can operate. There are a few countries where it would be illegal to start a WISP business. Some of the business regulations that a WISP might have to deal with are listed below.

- License to operate a WISP business.
- Permits to open the business premises.
- Permits to install the electrical equipment.
- License to operate communications equipment for specific frequencies.
- Licensed and insured technical staff including licensed staff who are qualified to climb towers and install antennas.
- Collection and reporting of telecommunications taxes.

The entrepreneur must investigate the local business regulation and legal requirements when planning to start a WISP business.

1.15. Summary

The key points that an entrepreneur should remember when considering starting a WISP business.

- Research potential customer interest for an Internet service in the planned area of operation.
- Research investment and operational cost information and calculate what value should be the charged per customer.
- Development of rate plans based on operating costs to divide the wholesale service between many retail customers and verify that potential customers are willing to pay the charge for the service.

- If the results of the first three steps are positive then sign an agreement with a wholesales Internet service provider (ISP) before spending money to build infrastructure.
- Find the investment capital required to build the network infrastructure to service the prospective customers and pay the wholesales Internet provider installation fees.
- Design the network with the capacity to deliver the Internet service to prospective customers and plan ahead for expansion of the network.
- Build out the basic network to provide a service for the first customers in order to begin generating revenue.
- Install the software tools required to manage the network and to add and bill customers.
- Develop operational procedures to support customers and maintain the infrastructure in good working order.
- Build a service organization to install the customer wireless equipment.
- Build a sales and marketing organization to attract customers and sell the service.
- Install software for monthly invoicing and follow up of receipts.

With the basic steps in place the ISP can start doing business and later plan the expansion to attract more customers.

2. Network technology for start-up WISP's

2.1. Data transmission over computer networks

Computer applications communicate over a computer network to a server (client server) or to another computer (peer to peer). A client computer can be a mobile phone, tablet, laptop or desktop. An example of a client-server application is the use of a browser to search the Google website for information. An example of a peer-to-peer application is a video and audio call between two client computers using Skype software.

When computers transfer data over a network the data file is divided into packets for transportation over the network using the TCP/IP protocol (Transmission Control Protocol / Internet Protocol). Data packets are transmitted sequentially until all the data has been transferred. The receiving computer then rejoins the packets in the correct sequence to recover the original file. The IP part of the protocol sends the packets over the network but there is no verification that the data packet arrived at the destination. Video streaming files are sent using the User Datagram Protocol (UDP), which uses the IP layer (UDP/IP) with no verification that the data packet arrived at its destination. This is done to increase the speed of the data flow while ignoring any transmission errors that might have occurred. The TCP part of TCP/IP uses the IP part to send the data but then requests an acknowledgement from the receiver that the data packet arrived without error. If the receiver replies that the data packet was good then the next data packet in the sequence is sent. If the receiver replied that the data packet had an error then the data packet is resent. If the receiver does not reply then the sender will retransmit the data packet after waiting for the duration of the time-out period. If the receiver still does not reply then the sender will generate an error message that the connection has failed.

All client and server computers have an Internet Protocol (IP) address, which the sender adds to the data packet and the sender also adds the senders IP address. Each device connected to the Internet must have a unique public IP that is not configured for any other device, and can be an IPv4 or IPv6 address.

The routers that manage the Internet network will forward the data packet until it reaches the destination IP address. The receiver can see the sender’s address IP address in the data packet and reply with an acknowledgement that the packet was received. The most common version of the Internet Protocol (IP) address is Ipv4, which has a 32-bit binary number for each IP and is usually written in a decimal format. An example of an IPv4 address is shown;

203.166.95.140

The Ipv4 address is written with four sets of decimal numbers of 0 to 255. This corresponds to four sets of hexadecimal numbers where each is 0 to FF. A 32 bit address gives 2^{32} addresses = 4,294,967,296 devices.

All available Ipv4 addresses were allocated some years ago, however blocks of IPv4 addresses can be purchased from brokers who are reselling IP addresses that were originally allocated to a service provider and are no longer required.

New devices that are connected to the Internet now have IPv6 addresses allocated. The IPv6 address is much larger with a 128-bit length, which gives 2^{128} addresses. An example IPv6 address is written as shown below using hexadecimal numbers;

30a0:0dcb:44a6:0000:0000:a815:df57:301b

When an ISP installs a router it will have an IPv4 address if the ISP has IPv4 addresses available to allocate to customers, and it will also have an IPv6 address. Network routers installed within the Internet backbone can route both IPv4 and IPv6 addresses.

Data is sent over the network in the form of data packets where each contains a block of data encapsulated with the information that is required to route the data packet through the Internet network to the destination. The IPv6 data packet is different to the IPv4 data packet. The WISP should not be concerned about the format of the data packet as this is handled by the firmware in computers, servers, wireless access points and routers, where all have the same TCP/IP protocol stack. The next diagram shows the format of an Ipv4 data packet that is prepared for transmission over a TCP/IP network.

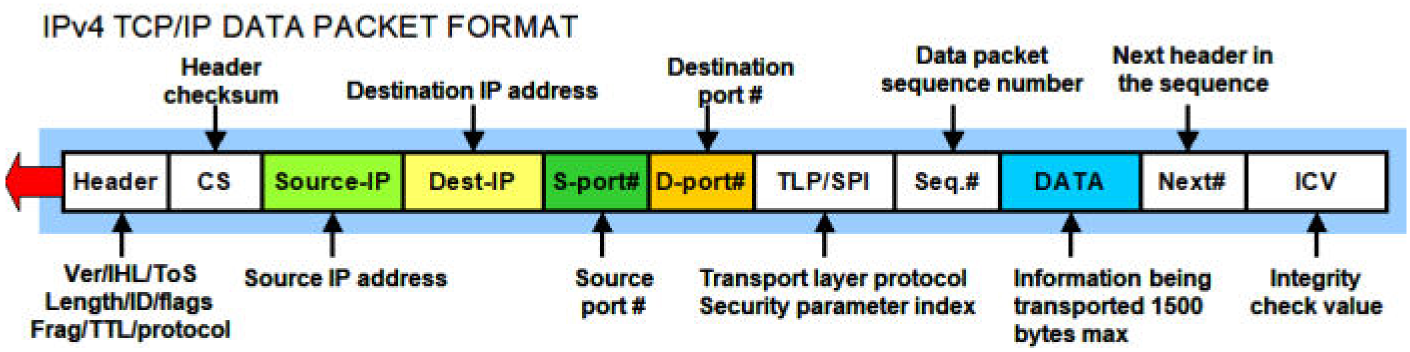


Figure 2.1.1 Data format of the IPv4 TCP/IP data packet.

A large file is divided into small data blocks where each has a maximum size of 1500 bytes. The data block is inserted into the data packet. Other information added to the packet includes the IP addresses that network routers will need to transport the data packet to its destination and verify that the packet arrived without error.

The destination IP address inserted into the data packet is the IP of the computer to which the message is being sent. Network routers will use the destination IP address to route the data packet to its destination computer. The source IP address is inserted by the sending computer and tells the destination device where to send the reply. There are three IPv4 ranges that are never used for public IP's and are used instead for private IP subnet ranges within the business or residential local area network (LAN). The LAN is connected to the public network with a router that provides Network Address Translation (NAT). The router translates or maps the range of private IP's used within the LAN to the public IP of the network to permit the data packet to be sent over the Internet. A data packet header must always have a public IP. The same private IP ranges are repeated in millions of local area networks (LAN's) around the world, but each LAN has a unique public IP when connecting to the Internet.

The three private Ipv4 ranges are listed below and these ranges are used within all business and residential networks.

- Class A subnet: 10.0.0.0 to 10.255.255.255
- Class B subnet: 172.16.0.0 to 172.31.255.255
- Class C subnet: 192.168.0.0 to 192.168.255.255

The ISP wholesale circuit will be delivered to the NOC with a public IP (Ipv4) or a small block of public IP's. When the WISP is designing and building the wireless distribution network that will connect the NOC to each subscriber the WISP has to make a decision about IP configuration, choosing the options listed below.

- Configure each customer CPE wireless/routers with a private IP, either class A, B or C allocated through a Dynamic Host Configuration Protocol (DHCP) process.
- Or purchase a block of public IP's (Ipv4 or Ipv6) and configure each CPE wireless/router with a static public IP.

This is of no concern to most customers; however there will be business customers who require their network to have a public IP because they are configuring remote access to their network or have staff connecting remotely via a service such as a VPN. If the customer CPE has a private range IP address then remote access can be configured by the WISP by installing a port-forward rule in the access control router. This will give the customer a public IP plus a port number for remote access to the customers network. The customer will also require a port-forward rule configured on the CPE router to provide remote access to devices or servers in the LAN.

In the USA a WISP can request an allocation of Ipv6 address by applying online to the American Registry for Internet Numbers.

https://www.arin.net/resources/guide/ipv6/first_request/

WISP's outside the USA should apply to the Regional Internet Registry that services Ipv6 requests for the geographic region where the WISP is based.

The source port number in the data packet is the address of the application program on the sending computer and the destination port number is the address of the application on the receiving computer. Some port numbers have been allocated for applications that are frequently used. Software developers of applications that communicate with other applications can use unallocated port numbers for the communication.

Examples of allocated port numbers are listed in the following table.

Protocol name	Port number(s)	Protocol description	Transport protocol
File Transfer Protocol (FTP)	20 and 21	Transfer files with verification to ensure that the file is transferred correctly.	TCP
Secure Shell (SSH)	22	Encryption protocol that ensures secure communications.	TCP and UDP
Secure File Transfer Protocol (SFTP)	22	File transfer that uses the SSH protocol for security.	TCP and UDP
Telnet	23	Console access to a terminal software.	TCP
Simple Mail Transfer Protocol (SMTP)	25	Transmit email messages to an email server.	TCP
Domain Name System (DNS)	53	Request to a DNS server to translate a domain name to an IP address.	TCP and UDP
Dynamic Host Configuration Protocol (DHCP)	67 and 68	Service requested by computer clients to allocate an IP address.	UDP
Trivial File Transfer Protocol (TFTP)	69	A simple file transfer that is used to upgrade firmware.	UDP
Hyper Text Transfer Protocol (HTTP)	80	Communication between a browser and a Web server.	TCP
Post Office Protocol 3 (POP3)	110	A client computer receives an email from an email server.	TCP
Network News Transport Protocol (NNTP)	119	Transport of data between a client computer and a network news server.	TCP
Network Time Protocol (NTP)	123	Access time information from a network time server.	UDP
Simple Network Management Protocol (SNMP)	161 and 162	Network device monitoring software will access a SNMP agent installed on each device.	TCP and UDP
Transport Layer Security (TLS)	443	Secure data transmission between two computers.	TCP
Hyper Text Transfer Protocol Secure. (HTTPS)	443	Secure encrypted communication between a client browser and a Web server.	TCP

Address Resolution Protocol (ARP)	3389	Resolve the network layer MAC address of a device.	TCP
Network Address Translation (NAT)	3022	Convert a public IP address to a private range IP address.	TCP and UDP
Real-Time Transport Protocol. (RTP)	5004	Stream video and audio from a server to a client.	UDP

Table 2.1.1. Examples of assigned port numbers and the applications to which they are assigned.

The communication protocols used by all applications are TCP/IP (Transmission Control Protocol/Internet Protocol) and UDP/IP (User Datagram Protocol/Internet Protocol). TCP/IP is a reliable connection where the reception and verification of each data packet is confirmed before the next packet in the sequence is sent. UDP/IP does not verify that the data packet has been received reliably. UDP is a faster method of communication however any transmission errors are not corrected. The TCP/IP and UDP/IP protocols are divided into layers, called a protocol stack. Each later is responsible for preparing the fields of the data packet for transmission. The TCP/IP and UDP/IP protocol stack is illustrated in the next diagram.

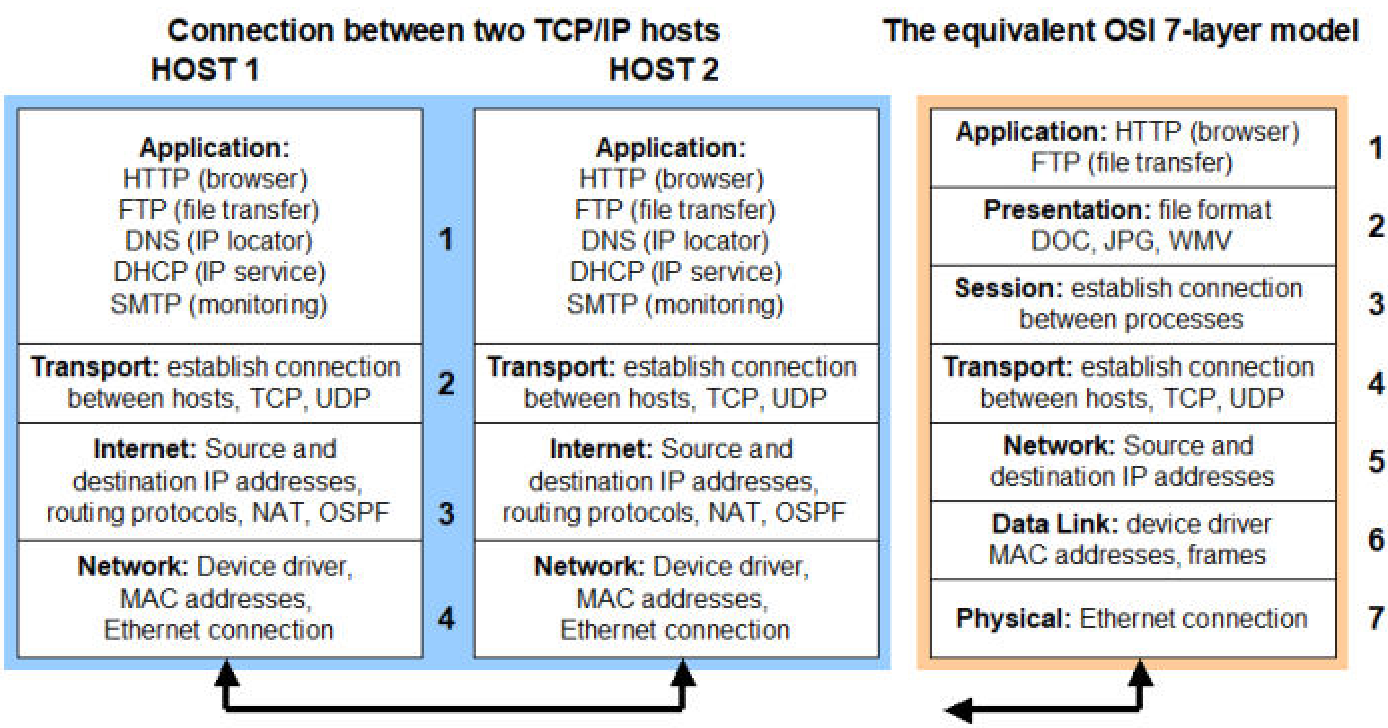


Figure 2.1.2: The TCP/IP protocol layer model compared with the OSI 7-layer model.

A conceptual communication protocol model called the OSI (Open Systems Interconnection) 7-layer model is compared with the TCP/IP protocol stack in the previous diagram. The OSI model provides a set of rules for a software developer who is designing a network product, which will assist the design inter-operability with other network products.

Several network processes are required for a client computer to connect to the network and to communicate with hosts in the network or in any part of the Internet. The first of these processes allocates an IP address to the client device so that it can communicate with other devices over the network. The process uses the Dynamic Host Configuration Protocol (DHCP), which is a client/server protocol. When a client is connected to a computer network the physical connection (e.g. Ethernet link light) indicates to the Ethernet interface that an IP must be requested. The client DHCP protocol sends out a DHCP request, which does not have a destination address as the client does not have information about the location of the DHCP server. There can be only one DHCP server in a network and that server will respond to all DHCP requests that are sent over the network. The DHCP server will issue one of the available IP addresses from a predetermined DHCP range. The start and end IP's of the range are specified in the server configuration. The DHCP server will respond to the client providing the IP address of the client, the gateway IP, the Netmask, and IP addresses for two DNS servers. The next figure illustrates the DHCP process.

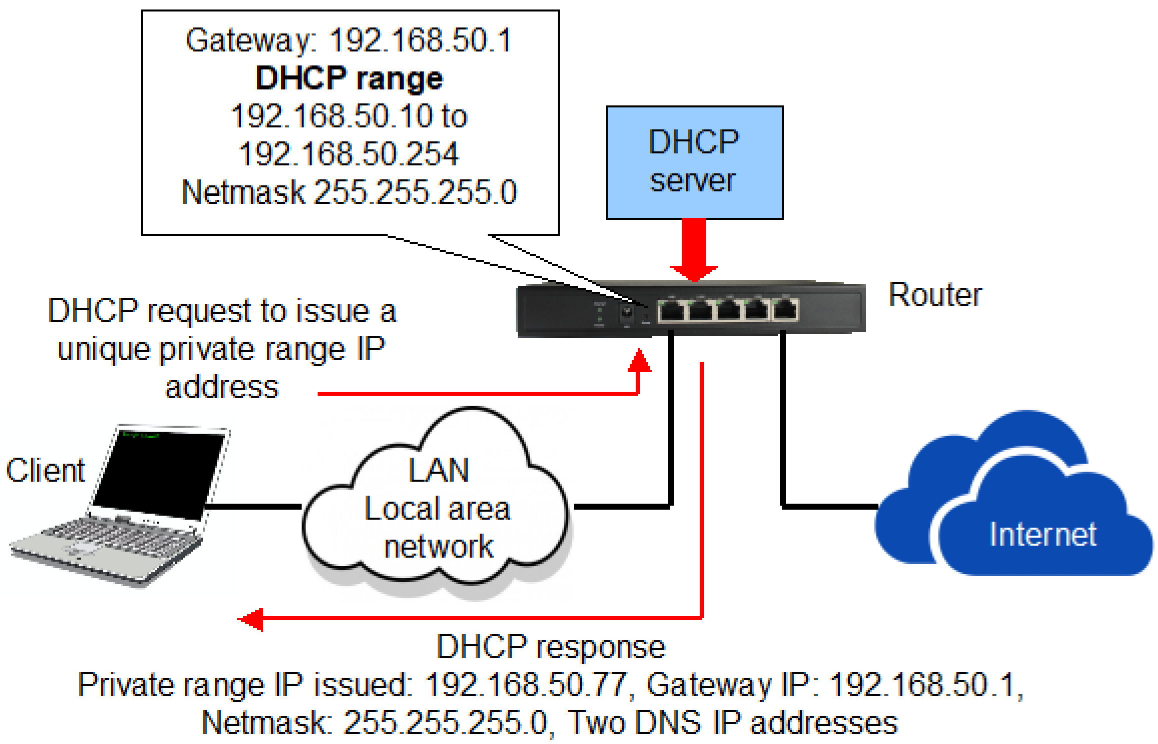


Figure 2.1.3: Client IP address allocation with the Dynamic Host Configuration Protocol (DHCP) process.

The server provides a gateway IP address, which the client will use as a destination address to communicate with the Internet, and a netmask, which the client will set in the network interface to determine the range of valid IP's that will communicate with the client over the network. The server will also provide a primary and secondary DNS server addresses. The client will configure the parameters in the device network interface. The DHCP server is usually incorporated within the router that connects the LAN to the Internet but can also be configured as part of a network server.

When the LAN subnet to which the client device is connected has a private IP range then a process is required to convert the client devices private IP to a public IP to permit communication over the Internet. The process is called Network Address Translation (NAT) and is required in every network that has private IP ranges. The next diagram illustrates the NAT'ing process.

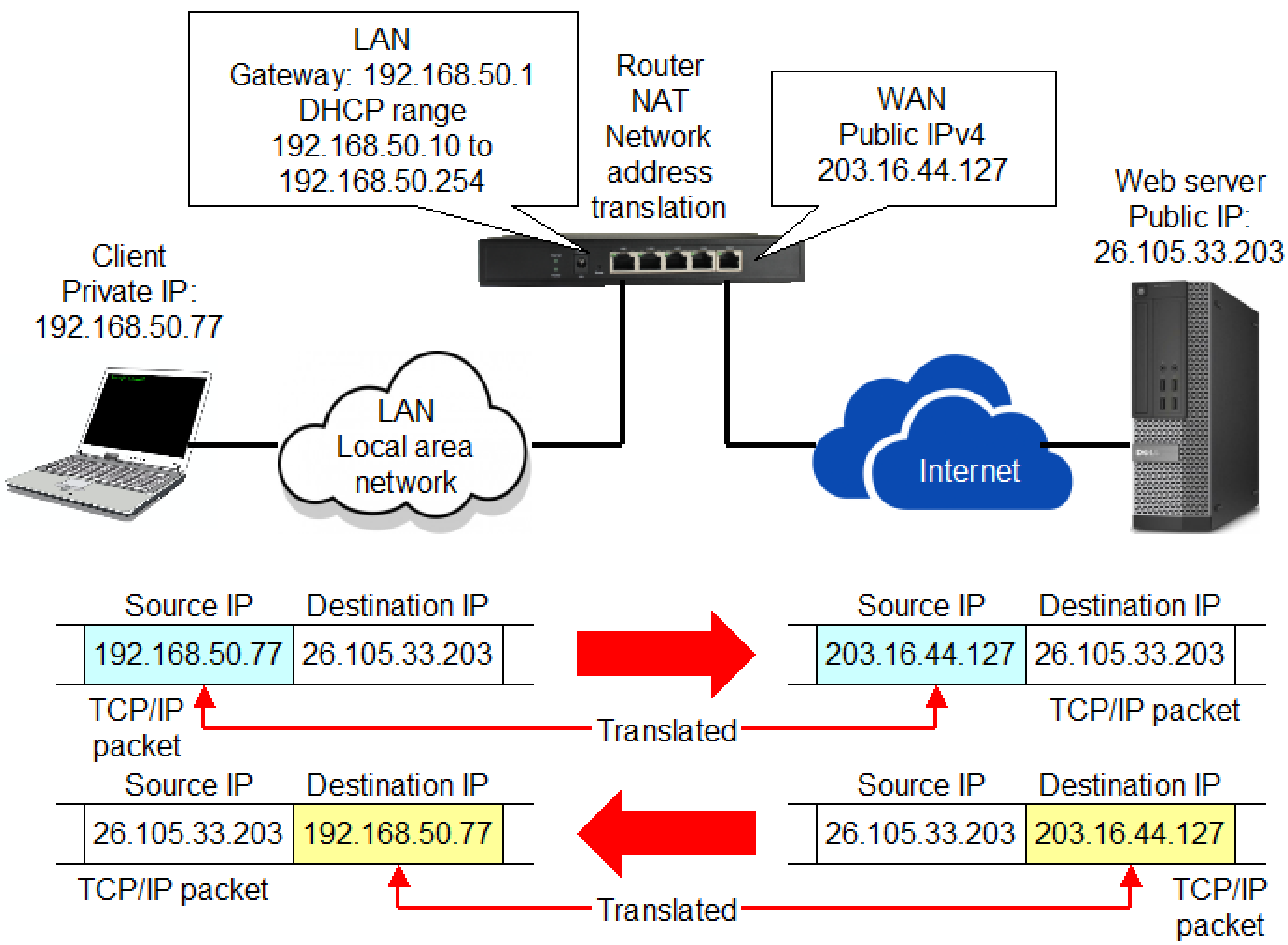


Figure 2.1.4: The router network address translation (NAT) process.

The client cannot use the private IP to communicate over the Internet, as the private IP will be duplicated in millions of LAN's. The client device must communicate with Internet services using the public IP of the LAN network. All devices in the LAN network will communicate outside the network with the same public IP. The router that connects the LAN to the Internet must translate the private IP of the client device to the public IP of the network when the client device sends a data packet to the Internet. When the router receives a reply from the Internet server the private IP of the device that sent the message must be restored to the data packet.

When the clients user opens a browser then the user will type the website domain name or complete URL into the browser. The Uniform Resource Locator (URL) is the address of a given unique resource on the Web server. Examples of the domain and URL are shown below.

www.guest-internet.com

https://www.guest-internet.com/docs/en

A process is required to permit the client to fetch the public IP address of the server represented by the domain name in order to access the requested web page. The browser uses the DNS protocol to send a request to a DNS server IP address that is provided by the DHCP service. The browser sends the domain name to the DNS server, which looks up the IP address of the domain in a translation table and then sends the IP address to the client. The client then sends a HTTP protocol request to the server's IP address to request the web site page.

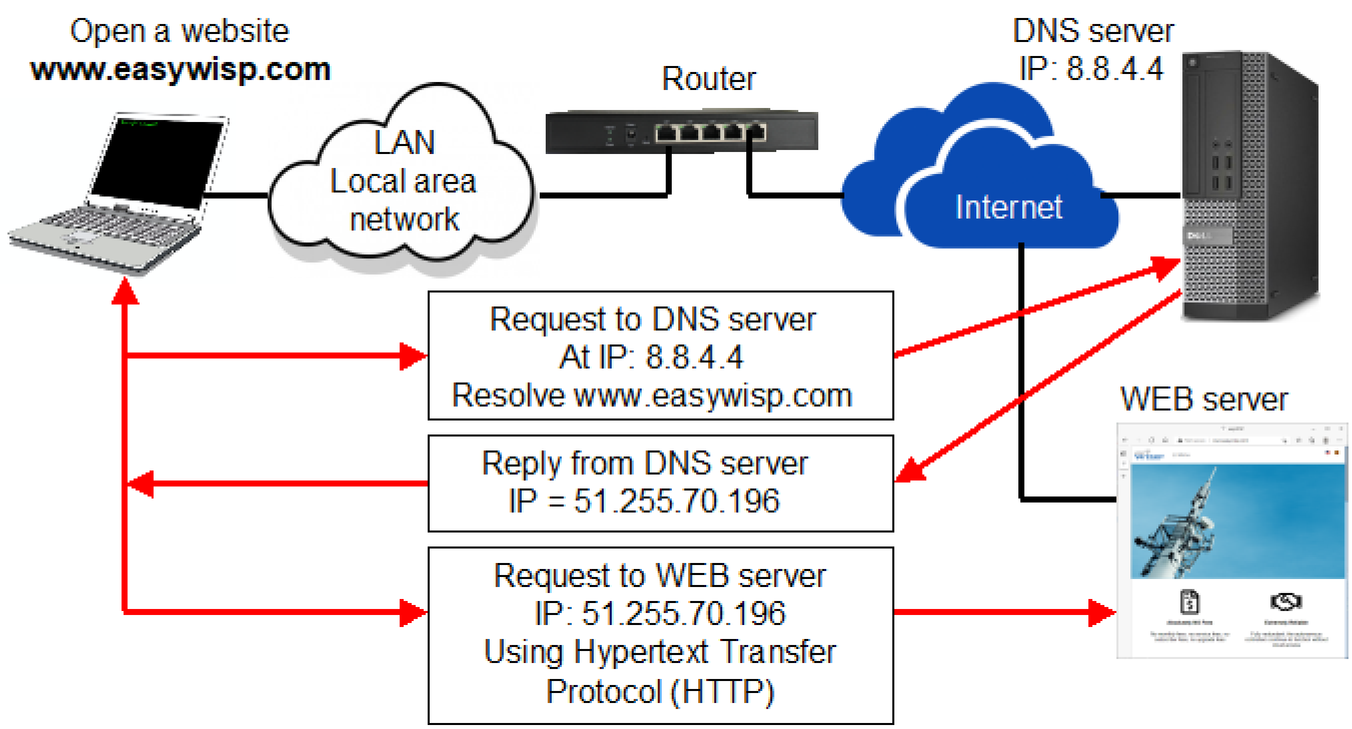


Figure 2.1.5: Using a DNS server to resolve a domain name to an IP address.

2.2. Wireless data network technologies

Wireless technology is in widespread use for data communications, principally because people want to use battery powered mobile computer devices, which include smart phones, tablets, and laptop computers. Most non-mobile desktop computers also connect via wireless. There are two major wireless technologies for data communications.

- GSM and CDMA mobile phone standards, which evolved to become the 4G LTE (long term evolution) standard and now 5G.
- IEEE 802.11 WiFi standard.

Mobile phone networks are the major user of wireless technology and frequency allocation. A significant proportion of people have access to mobile phones. 4G LTE has the following characteristics.

- The network topology is host-client, where the host (cell phone tower) can communicate with one or many clients. A single host to client LTE connection is called a point-to-point (PtP) link. A LTE connection of one host to multiple clients is called a point to multi-point (PtMP) connection.
- The data connection is peer to peer, that is one client calls another client using a numerical code (telephone number), or else one client connects to a network service using a numerical code (IP address).
- The transmission frequencies are licensed by the appropriate government department (FCC in the USA) and leased out to carriers through an auction process. This insures that the band of frequencies that a carrier pays for are exclusive to that carrier so there will be no interference, ensuring a good quality connection. If the carrier finds interference then it will call the government entity responsible for radio frequency transmission (FCC in the USA) to confiscate the offender's equipment.
- All equipment that is used for wireless communications by the carrier must be approved for use by the government entity responsible for radio frequency transmission (FCC in the USA). Obtaining approval is the responsibility of the equipment manufacturer.
- The carrier leases a band of licensed frequencies for the communication service, however the carrier can choose the method of communication using those frequencies. Some parts of the world use 3G GSM, while the widely used method currently in many countries is 4G LTE. Many carriers are now migrating networks to 5G which offers faster data speeds. Each improvement allows the carrier to connect more customers using the licensed frequencies bands and provide each client with a higher data communications rate.
- Cell phone tower transmitters have a relatively high transmission output measured in Watts (50 to 100 Watts), which provides a range of several Km to each client device from the tower, even though the client device is relatively low powered (0.5Watt) and has a very poor antenna that is not directional.
- Currently there are 88 frequency bands that are part of the LTE specification, which range from 450MHz up to 5900MHz. However not all bands are available

in all countries, with an average of 20 bands available in each country, chosen by the government. Therefore a mobile phone that works in one country may not work in another country, so mobile client devices are not portable between countries. While the low frequency bands below 1000MHz have good penetration through obstacles and into buildings, the high end of the frequency ranges in the 2000MHz to 5000MHz range have poor penetration into buildings which causes client connection problems. Some examples of LTE frequency bands are shown in the following table.

LTE Band Examples

LTE Band Number	Frequency	Bandwidth (MHz)
LTE Band 43	3600 - 3800 MHz	200
LTE Band 44	703 - 803 MHz	100
LTE Band 45	1447 – 1467 MHz	20
LTE Band 46	5150 – 5925 MHz	775

Table 2.2.1. Examples of LTE band frequency allocation.

In the early 2000’s when 1G and 2G mobile phone networks were the standard of mobile phone data communication, a high-speed data communication standard was developed called IEEE 802.16 (WiMAX), to operate on licensed frequencies. However WiMAX became redundant as GSM and subsequently LTE technologies developed to provide faster data speeds and passed WiMAX in terms of performance. Many WiMAX networks were built for fixed broadband applications but were subsequently replaced with LTE technology due to the superior performance of LTE.

IEEE 802.11 WiFi standard network products have developed to become a world wide standard due to the use of unlicensed frequencies that the telecom companies could not use. The primary frequency of 2.4GHz is the frequency used by microwave ovens to heat up food. 2.4GHz is the frequency at which water molecules absorb radio frequency energy and heat up so it has limited use outdoors when raining. The main applications for WiFi are indoors for short distance local area networks at low transmission powers. The IEEE 802.11 WiFi standard has the following characteristics.

- The network topology is host-client, where the host (the wireless access point) can communicate with one or many wireless clients. A single host to client WiFi connection is called a point-to-point (PtP) link. A WiFi connection of one host to multiple clients is called a point to multi-point (PtMP) connection.

- The data connection is peer to peer, that is one client communicates with another client or else one client connects to a network service such as a Web server using a numerical code (IP address).
- The principle transmission frequencies are un-licensed but controlled by the appropriate government department (FCC in the USA). This means that the un-licensed band of frequencies are subject to interference from many other sources; not only other WiFi devices but from cordless phones and garage door openers to name a few. The data connection is generally poor quality in a dense urban area however it is better in a rural area. The 5.8GHz band usually has less interference than the 2.4GHz band. The requirement to use unlicensed frequencies is that the device must not cause unnecessary interference with other devices. WiFi can also be used by WISP's on licensed frequencies in order to minimize interference. The WISP must get approval from the appropriate government department (FCC in the USA) to use a licensed frequency and pay a subscription (usually annually) for the use of the frequency band.
- All equipment that is used for WiFi communications by the carrier must be approved for use by the government entity responsible for radio frequency transmission (FCC in the USA). This approval is the responsibility of the equipment manufacturer.
- The WiFi equipment manufacturer can choose the method of communication that is specified by the WiFi technical standard. New transmission standards are added periodically with higher data rates that are always backwards compatible with earlier standards.
- WiFi wireless devices have a low transmission output measured in Watts (0.1Watt in the EU to 1 Watt in the USA), which provides a range of a few hundred meters maximum to each mobile client device from the wireless access point. By adding a high gain directional antenna the maximum communications distance can be increased to a few tens of Km's.
- The WiFi standards have been universally adopted and so a WiFi device will work with a network in any country of the world.
- There are two principal unlicensed frequency bands that are part of the WiFi specification, which are 2.4GHz and 5.8GHz. Each frequency band is divided into a number of channels. The frequency ranges of 2.5GHz and 5.8GHz have poor penetration into buildings and are for line-of-sight (LoS) communication only.
- Other unlicensed frequency bands are available in some countries. The unlicensed frequency bands are part of the ITU (International Telecommunications Union) agreement of which most countries are members. The unlicensed bands are called the ISM (industrial, scientific and medical) bands.
- The following table shows the unlicensed ISM bands that can be used by WISP's for WiFi communications. Not all of these bands are available in all countries and each country sets the maximum permitted power of the radio frequency (RF) output.

ISM (industrial, scientific and medical) frequency bands available for unlicensed communications

Frequency range		Center frequency	Bandwidth	Availability
902 MHz	928 MHz	915 MHz	26 MHz	Not available in all countries
2.4 GHz	2.5 GHz	2.45 GHz	100 MHz	Worldwide
5.725 GHz	5.875 GHz	5.8 GHz	150 MHz	Worldwide
24 GHz	24.25 GHz	24.125 GHz	250 MHz	Worldwide
61 GHz	61.5 GHz	61.25 GHz	500 MHz	Not available in all countries

Table 2.2.2. ISM frequency bands for unlicensed data communications.

The table shows two unlicensed very high frequency bands at 24GHz and 61GHz. These bands are available for very high-speed point-to-point wireless data connections over shorter distances. The wireless equipment for these frequencies is expensive but if a very high bandwidth point-to-point backhaul to the PtMP tower is required then these frequencies can be used.

2.3. Wireless WiFi network technology for WISP's

The technology that most WISPs' will use to build out wireless networks is IEEE 802.11 WiFi operating on the unlicensed frequencies of 2.4GHz or 5.8GHz. IEEE 802.11 WiFi equipment has lower cost than equipment for other frequencies as the components are manufactured in large volumes for the consumer market and therefore have the lowest cost. In addition there are no fees to use the unlicensed spectrum. The disadvantage is that there are many devices operating with the same frequencies and so the communication is subject to interference.

Before a wireless device can be used the competent authority in each country must certify it. In the USA a product must have FCC certification, in Europe a product must have a CE registration. It is the product manufacturers responsibility to obtain certification.

Transmissions at frequencies of 2.4GHz and 5.8GHz can be blocked or attenuated by walls or trees. For this reason transmissions at these frequencies must be line-of-sight, which means that the client antenna must have visibility of the host antenna.

The operating configurations that WISPs use are point-to-point (PtP) and point to multi-point (PtMP). The PtP configuration has one host and one client and is used to build a wireless data link between two points. This wireless link can carry data over several Km and replaces a copper or fiber cable for a much lower cost. The PtMP configuration has one host (wireless access point) and many clients (the client premise equipment or CPE). The standard has no limit specified for the number of clients that can connect to one host however there is a practical limit determined by the performance of the host wireless access point. The practical limit may lie between 50 and 300 clients connected to one wireless access point.

The WiFi specification describes three wireless modes of operation, listed below.

- Infrastructure mode.
- Ad hoc WiFi direct.
- Multiple access points.

Infrastructure mode permits two clients to communicate via the host wireless access point. This mode should be prevented for a WISP installation as it is not desirable for two clients to communicate. The only communication that should take place is between one client and an Internet client or website.

The ad hoc mode permits two clients to communicate without the data passing through the host wireless access point. This mode of operation is also undesirable for a WISP network and generally not possible as a large distance separates two clients, each with antennas pointing at the PtMP host wireless access point. This mode of operation is suitable only for a business local area network where client devices are in close proximity.

The multiple access point mode is appropriate for WISP mobile broadband networks where it is desired that the mobile client can move between different wireless access point sites. To implement mobility it is necessary that all wireless access points broadcast the same identifier called the SSID (Service Set Identifier) and have the same security settings (encryption key) so that the client device will connect to the wireless access point when the broadcast is detected.

Governments impose signal strength limits for each frequency band, which results in range limitations for users of the unlicensed frequency bands. In the USA the peak antenna power (Effective Isotropic Radiated Power - EIRP) must not exceed +36dBm, which translates to 4 Watts of RF output. Countries in the EU have a much lower maximum power level of +20dBm, which is 100mW maximum transmitter power output.

For comparison, a home wireless router will have a power output of 50mW to 100mW. A wireless access point designed for outdoor use in the USA will have a transmit power from 250mW to 1Watt, and will have an antenna with a gain of 5 to 10 dB. When the WISP purchases equipment that is FCC or CE approved then the product will function within the legal requirements of the country in which it was purchased.

Wireless equipment for the 2.4GHz band will cost less than equipment for the 5.8GHz band due to the popularity of the 2.4 GHz band for wireless LAN networks. The cost of dual band wireless equipment (2.4GHz and 5.8GHz) is higher, however dual band wireless equipment will provide the best performance for throughput and increase number of subscribers that can be connected.

Each band is divided into channels and the wireless access point is configured to transmit on one of the channels. A wireless access point operates only on one channel, however a wireless access point with a high data rate will occupy several channels of bandwidth. Some wireless access points can move between channels to avoid interference. When a client device is configured the technician will scan all channels and identify the correct wireless access point for the wireless connection.

The figures show the channels for the unlicensed 2.4GHz and 5.8GHz bands that are permitted in many countries.

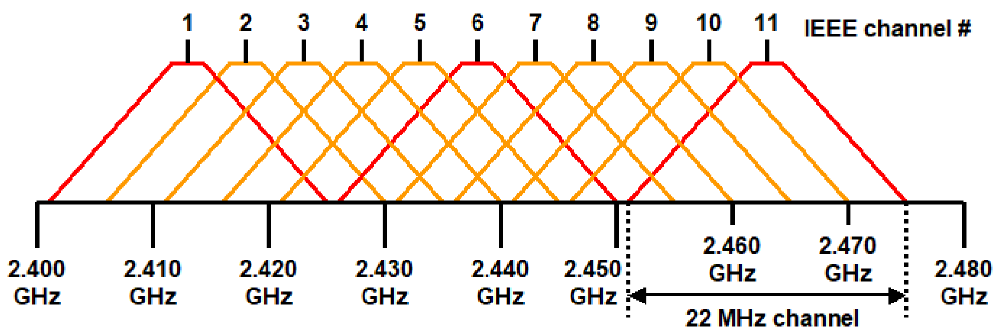


Figure 2.3.1. IEEE 802.11 overlapping channels in the 2.4 GHz band.

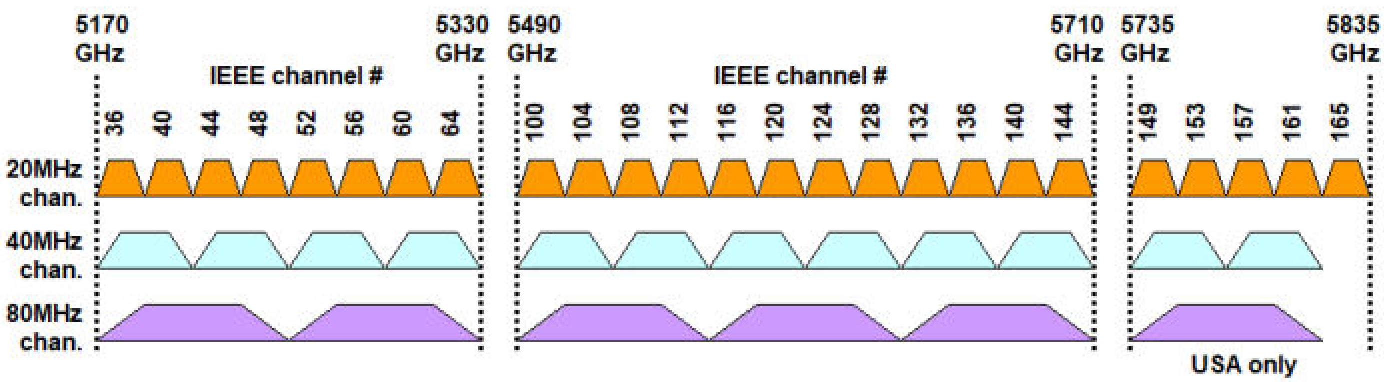


Figure 2.3.2. IEEE 802.11 channels in the 5 GHz band.

Each country has a number of licensed bands that are available for telecommunications companies to use, for either point-to-point (PtP) or point-to-multipoint (PtMP) communication. The advantage of the licensed frequency bands is that there will be very little interference and so the quality of the service provided to subscribers will be much higher. The disadvantage is that there will be two additional costs. The first is the fee that the government will charge for using the licensed band, which is likely to be an annual fee. The second cost occurs because wireless equipment for licensed bands is much more expensive than equipment for unlicensed bands. This is because the volume of equipments manufactured for licensed bands is much smaller therefore manufacturers cannot get the cost advantages of large-scale production.

The IEEE 802.11 standard is continually expanding to add new data encoding methods that enable the allocated frequency bandwidth to support communication at higher data rates. As each standard is released it is backward compatible with the previous standards. The evolution of WiFi technology is illustrated in the following table.

Development of Wi-Fi standards				
WiFi Generation	**IEEE Standard**	**Maximum data rate**	**Year approved**	**Frequency**
Wi-Fi 1	802.11	1 to 2 Mbit/s	1997	2.4 GHz
Wi-Fi 2	802.11b	1 to 11 Mbit/s	1999	2.4 GHz
Wi-Fi 3	802.11a	6 to 54 Mbit/s	1999	5 GHz
Wi-Fi 3E	802.11g	6 to 54 Mbit/s	2003	2.4 GHz
Wi-Fi 4	802.11n	72 to 600 Mbit/s	2008	2.4/5 GHz
Wi-Fi 5	802.11ac	433 to 6933 Mbit/s	2014	5 GHz
Wi-Fi 6	802.11ax	600 to 9608 Mbit/s	2019	2.4/5 GHz
Wi-Fi 6E	802.11ax	600 to 9608 Mbit/s	2019	6 GHz

Table 2.3.1. The evolution of IEEE 802.11 WiFi standards.

IEEE 802.11 data transmission is half duplex, this means that data can travel in only one direction at one time, either the host wireless access point is sending a message to the client, or else the client is sending a message to the host wireless access point. Both cannot send messages concurrently. The network access method is called CSMA/CD (Carrier-sense multiple access with collision detection), which prevents one transmitter interrupting another transmitter. If an interruption occurs it is called a collision and results in each transmitter having to restart the transmission, which reduces the transmission bandwidth. In addition with PtMP installations the bandwidth available is shared between all clients, only one client can communicate with the PtMP host at one time.

Data communication between the host and the client is encrypted for security. The popular encryption algorithm is WPA2 (WiFi Protected Access II). One encryption key is configured for the host, and each client is configured with the same encryption key. A version of WPA2 called WPA2-enterprise has greater security. Each client has a unique credential and the host verifies the credential by communicating with a RADIUS database. RADIUS is open-source software that has become a standard for client authentication. RADIUS authentication is also used with a popular authentication protocol called PPPoE (Point-to-Point Protocol over Ethernet) that many WISP's use.

There is one exception where the wireless transmission is not encrypted; this is the public WiFi Internet Hotspot configuration. As anonymous users connect to the Internet Hotspot then if the transmission were encrypted the key would have to be given to everyone, which negates the purpose of a secret key. The Hotspot wireless access point is therefore not encrypted and any mobile device within range of the wireless access point can connect to it.

Wireless clients and hosts have additional parameters, called modes of operation that describe how the data traffic is managed through the device.

- Access point bridge mode.
- Access point router mode.
- Wireless repeater.
- Wireless Distribution System (WDS).
- Mesh wireless network.
- Client wireless in router and bridge mode.

The access point bridge mode of operation connects the wired Ethernet port of the wireless access point (LAN) to the wireless port (WLAN) with no modification of the data flow. All requests such as DHCP are passed back to the router behind the wireless access point.

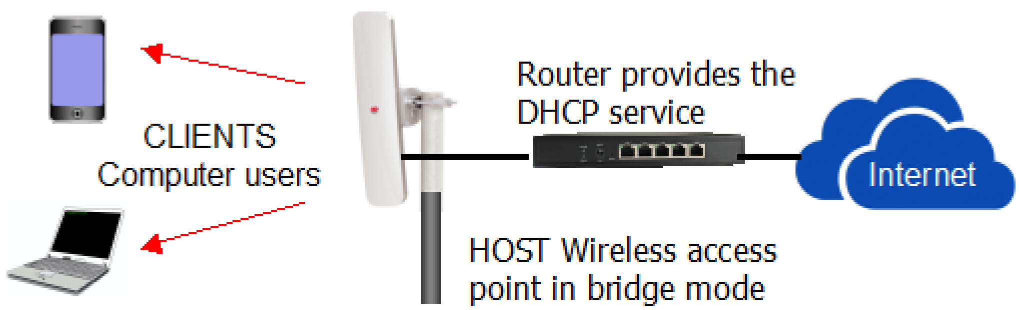


Figure 2.3.3. Wireless access point bridge.

The access point router mode of operation provides a DHCP (Dynamic Host Configuration Protocol) service for the wireless port (WLAN), which issues IP addresses to all clients that connect to the wireless port. The WLAN DHCP service therefore has a private subnet of IP addresses. The wireless access point provides network address translation (NAT), which translates the IP addresses of data packets on the WLAN port to the IP address of the LAN port. When a data packet is received at the LAN port it is routed to the correct WLAN client. The wireless router is a popular product for homes and small offices.

Figure 2.3.4. Wireless router.

The wireless repeater mode of operation does not use the LAN port. For this mode of operation data packets received by the WLAN port are retransmitted. As one wireless port is used for both reception and transmission, which cannot occur concurrently, the retransmission of data packets reduces the speed to half of the original transmission value. The WISP may find the repeater mode useful in a fringe area of coverage where it is necessary to boost the signal strength. The WISP can configure a client wireless together with a host wireless access point, each set to a different frequency, as a repeater configuration by connecting the two LAN ports so that the data speed is not reduced.

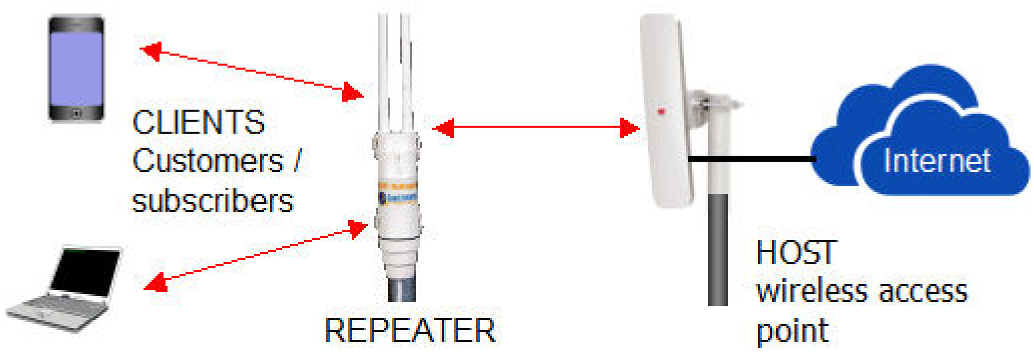


Figure 2.3.5. Wireless repeater.

The Wireless Distribution System (WDS) mode permits the connection of multiple Access Points in the point-to-multipoint bridge mode, connected via point-to-point wireless links and is essential for network configurations where the client MAC address must be passed over a wireless distribution network to the router for the authentication process. WISP's will be using a wireless distribution network to connect PtMP towers back to the location where the wholesale circuit is installed, called the network operations center (NOC). The WISP may be using the MAC address of the client to authenticate that client at the NOC.

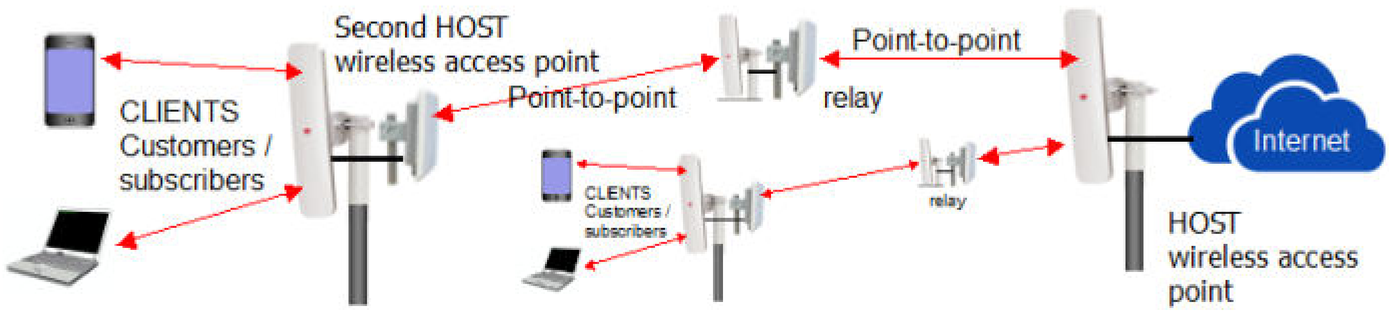


Figure 2.3.6. Wireless distribution network.

The mesh mode of operation combines the wireless repeater mode with routing services. One or more wireless access points are connected to LAN cables and then communicate with other mesh wireless repeaters through several hops to the client. The performance of a mesh network degrades in function of the number of hops between the client and the wireless access point connected to the LAN. The WISP may find that the mesh network has applications when building the wireless network, which connects clients to the PtMP tower.

Figure 2.3.7. Mesh network.

The last wireless configuration is the client wireless, called the CPE (customer premise equipment). This client is installed at the customer premises and many CPE's communicate with one point-to-multi-point wireless access point. The CPE can be configured as a router in which case the customer computer or wireless router receives an IP address from the CPE. Alternatively the CPE can be configured as a bridge in which case the customer computer or wireless router receives an IP address from the router behind the wireless access point.

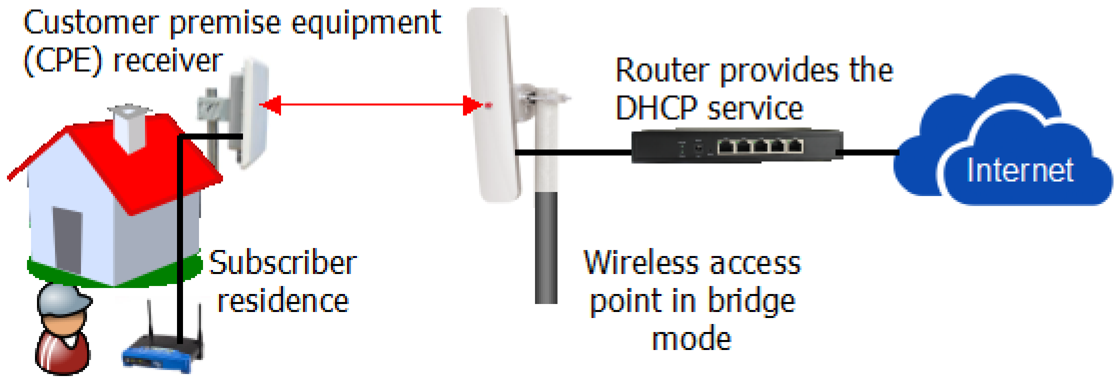


Figure 2.3.8. Customer premise equipment (CPE); wireless configuration.

2.4. Product technology for WISP wireless networks

WISP's build wireless networks with products that are designed specifically for the WISP market. Generally WISP products are considered to have higher performance and are more reliable through the use of high quality components, than products for the consumer market. They are also more expensive. All products for wireless networks are designed around chips that implement the IEEE 802.11 standard. As of writing this book there were 75 manufacturers of wireless chips and chip sets for the IEEE 802.11 standard. Most chips and chip sets are designed for the high volume consumer electronics market and provide basic IEEE 802.11 functionality. The consumer market includes all types of computers and mobile devices, home and office wireless routers and devices such as gaming consoles. Intel for example manufactures wireless chips for the consumer market in addition to processors. The wireless chipsets have processors (CPU's) and the features of the wireless devices are implemented in software.

WISP wireless products require more features than those developed for consumer electronic products. They have a higher radiated power for longer communications distances and have more configurable transmission parameters, therefore the chip set options for WISP product manufacturers are limited. WISP wireless product manufacturers differentiate their products from competitors that use the same chipset by developing software for the products that enhances the product performance and functionality.

Most WISP wireless products use one of three chipsets, the processors use either the MIPS or the ARM core, which are both reduced instruction set (RISC) designs. ARM core processors are used exclusively in mobile phones due to the low power consumption of the design. The ARM core is more popular because it provides higher processing performance than the MIPS core.

- Qualcomm Atheros: considered to have the most advanced technology of all manufacturers and are selected by the majority of WISP wireless manufacturers. Qualcomm also supports a wireless management software product called openWRT, which provides standard management software for all wireless products that use Qualcomm Atheros chips. The Qualcomm Atheros chips also have premium pricing so products with these chips are slightly more expensive than other products. Qualcomm Atheros chips are also used in consumer products.
- MediaTek Ralink: less popular than Qualcomm Atheros for WISP products. Lower cost chips for the products that don't require maximum performance and offer a price advantage. MediaTek Ralink chips are also used in consumer products. The openWRT software is available for products that use the MediaTek Ralink chips.
- Broadcomm: very popular for consumer products but less popular than Qualcomm Atheros for WISP products. Lower cost chips for the products that don't require maximum performance and offer a price advantage. The openWRT software is available for products that use the Broadcomm chips.

All wireless devices require configuration before they can operate in a wireless network. Each wireless product brand has many different configuration parameters and they are all different in the way that the parameters are configured using the device firmware. A list of common parameters is presented here with an explanation of each one. The manufacturer usually provides a manual explaining the configuration process.

- Most wireless devices have an IP address with a default HTTP port of 80 that is used to access the User Interface (UI) via the computer browser. The wireless device LAN port is connected to the computer LAN port for configuration. The computer LAN port should be configured for a static IP address in the subnet range of the wireless device LAN IP.
- The LAN port configuration UI IP address and port number can be changed in the UI configuration for values that are compatible with the target network.
- Some wireless devices (e.g. Ubiquiti Unifi) do not have a UI, instead software is provided to install on a computer, which is then used to configure the wireless device. Ubiquiti also has a configuration device that has a UI, which in turn accesses the wireless devices to configure them.
- Configure the wireless WLAN port for wireless parameters; transmission bandwidth, etc. Leave these at factory default when starting.
- Select the product to operate as a host (access point mode) or as a client (client mode).
- When configured in access point mode, set the broadcast name (SSID) and select the transmission channel.
- Select the encryption type if used, no encryption for Hotspot, WEP, WPA2, WPA2-enterprise, and set the encryption password. If encryption is WPA2-enterprise then the network must have a RADIUS server for authentication.

- Select bridge or router mode operation for either access point mode or client wireless mode.
- When configured in access point mode, and the access point is in router mode configure the access point Ethernet WAN port for DHCP client or static IP.
- When configured in access point mode, and the access point is in router mode configure the WLAN port for DHCP service.
- When the wireless client is configured in router mode then configure the LAN port for DHCP service.
- When the wireless client is configured in router mode then configure the wireless WLAN port for static IP or DHCP client.
- When configured in wireless client mode scan for AP's and select the AP to connect with.

Other configuration parameters are added by manufacturers for specific reasons, one example is to improve data throughput over a point-to-point link.

2.5. Fixed broadband Internet service

The fixed broadband wireless service provides a data connection from a central point, the PtMP wireless access point, to each customer's premises. The wireless transmission is encrypted using WPA2 or WPA2-enterprise. The customer premises has a fixed antenna installation, which is called the customer premise equipment (CPE) because this was the name given to the product by telecom companies who connected their client's last mile using wireless. The advantage of the customers fixed antenna installation is that a high gain directional antenna can be installed to give a long range of communications to the PtMP antenna; the distance can extend to several Km's. The distance between the two antennas must have line-of-sight with a clear space around the line-of-sight. Any obstacle such as a tree or building will block the transmission. The diagram illustrates the fixed broadband wireless infrastructure installation.

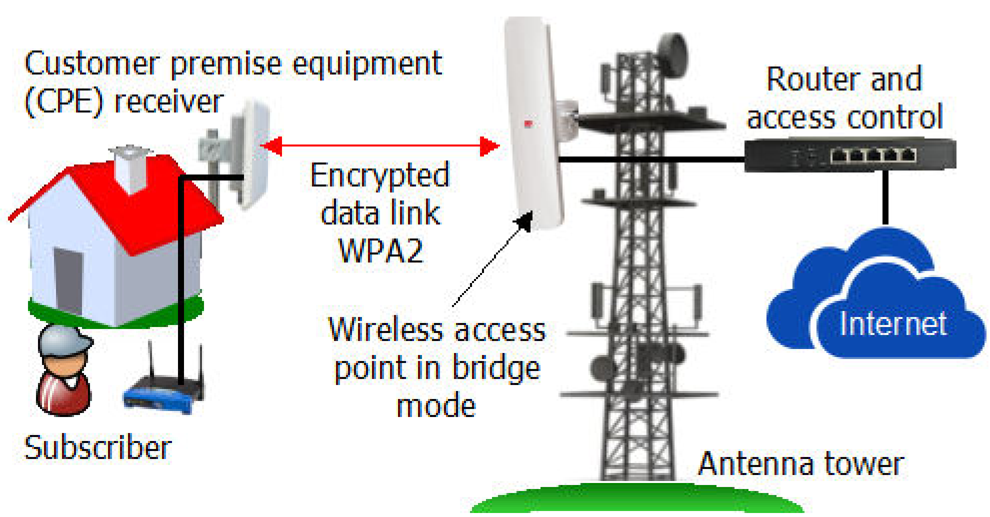


Figure 2.5.1. Fixed broadband wireless infrastructure.

Customers of the Internet service connect wirelessly to a point-to-multi-point (PtMP) wireless access point (WAP), which in turn connects to an Internet service via the access control router. The wireless access point can connect multiple customers simultaneously and this is the reason that it is called point to multi-point. The number of customers that can connect to a wireless access point depends on the performance of the product, on the wireless frequency bands that the wireless access point is using, and on the speed of the Internet connection.

It is important to install the wireless access point antenna at a point where it is visible for the maximum number of users so that they have line-of-sight to the antenna. The reason that users must have line-of-site to the antenna is that the signals of the two unlicensed frequency bands of 2.4GHz and 5.8GHz are blocked by buildings and trees. The wireless access point antenna is installed at a high point to give the maximum visibility. This might be on the roof of a tall building, on an antenna tower, or on a hillside overlooking a town. Antenna installations are illustrated in the following figures.

Figure 2.5.2. Wireless access point antenna installed on a building roof.

Figure 2.5.3. Wireless access point antenna installed on an antenna tower.

Figure 2.5.4. Wireless access point antenna installed on a hillside overlooking a town.

The PtMP antenna is installed on a tower or building roof and is connected to an Internet circuit at that location if available. If there is no Internet circuit at the PtMP tower site then the tower is connected back to the network operations center (NOC) site using a point-to-point wireless link. A wholesale service provider installs a copper or fiber high capacity trunk circuit at the NOC site. The next figure illustrates a PtP parabolic antenna installed at the PtMP tower providing the wireless backhaul connection.

Figure 2.5.5. PtMP tower with parabolic backhaul antenna for the PtP data link to the NOC.

In some PtMP tower installations it is not possible to have one point-to-point link from the tower to the network operations center (NOC), either because the distance is too great or else the terrain does not permit a line-of-sight connection. In this case several links or hops are used to connect the PtMP location back to the point where the Internet circuit is available at the network operations center. The Intermediate antennas in the chain are called relays or repeaters and consist of two directional antennas, each with a wireless access point, one configured as a host and the other as a client and each configured for a different channel to avoid interference. There is a limit to the number of hops as each introduces a transmission delay, called latency, and can also reduce the bandwidth available due to distortion of the transmission signal.

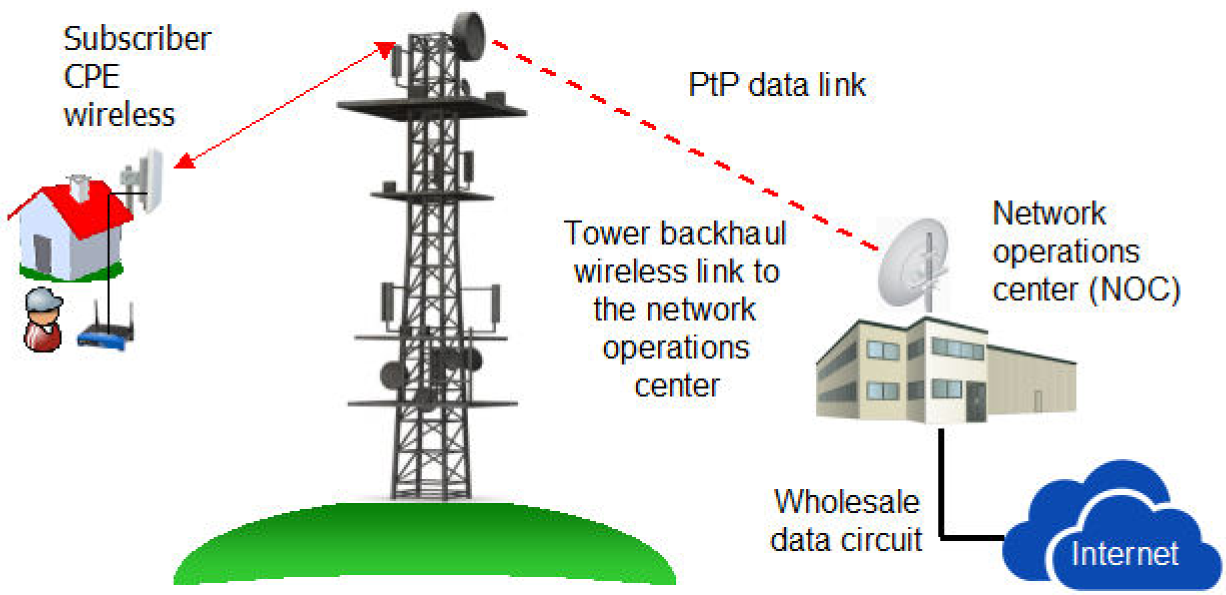


Figure 2.5.6. Tower wireless backhaul connection to the NOC building using a point-to-point wireless link.

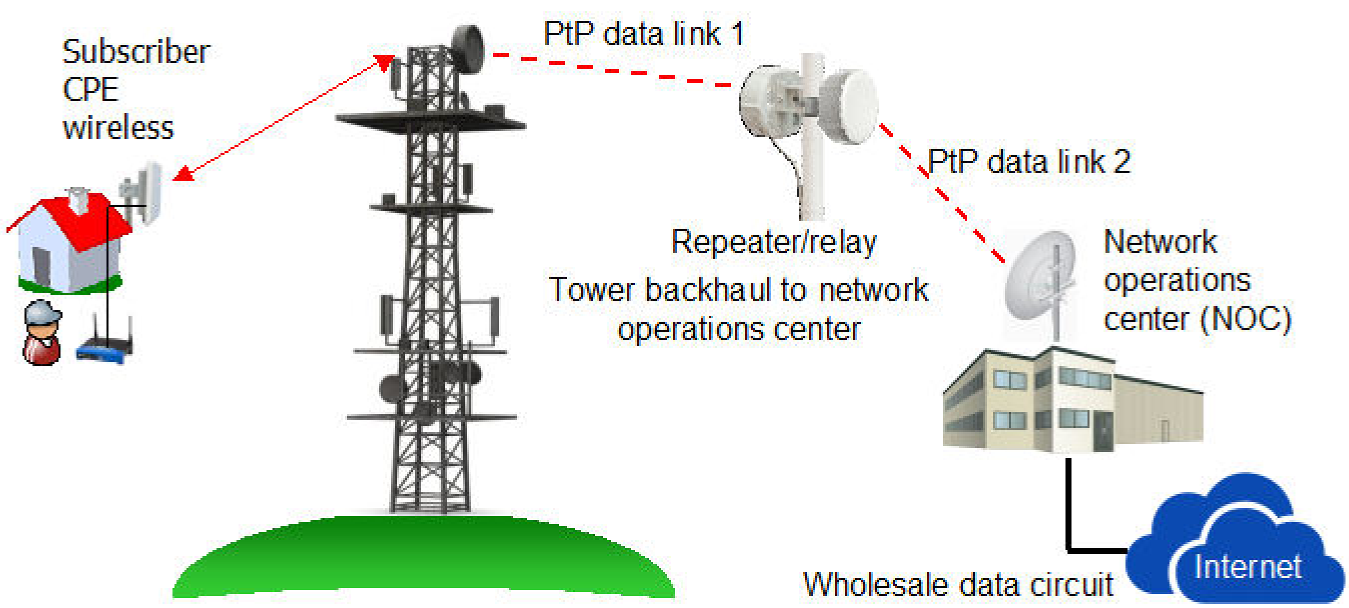


Figure 2.5.7. Tower wireless backhaul connection to the NOC building with two point-to-point wireless links via a wireless relay/repeater.

The next figure shows the installation of a relay/repeater at a point between the PtMP antenna tower and the NOC.

Figure 2.5.8. Relay/repeater antenna to extend the distance between the PtMP tower and the network operations center and for non-line-of-sight connections.

The fixed broadband customer Client Premise Equipment (CPE) can be located several Km from the Internet service provider PtMP antenna with a line-of-sight view of the PtMP antenna because a wireless receiver with a high gain directional antenna is installed on the roof of the customer's premises.

Some technical characteristics are listed below for the CPE wireless installation with a directional antenna.

- The antenna must be installed securely at a high point on the building so that wind or other climate effects do not cause movement of the antenna.
- The antenna must have line-of-sight visibility to the transmitting antenna with clearance around the line-of-sight view (Freznel zone).
- The antenna position must be carefully adjusted for maximum signal strength using a signal strength meter incorporated into the CPE software.
- Outdoor Ethernet cable connects the CPE to the equipment inside the building. The Ethernet cable will carry the CPE data and also provide the CPE with power (Power over Ethernet).

Figure 2.5.9. CPE antenna installed on the roof of a subscriber building.

The wireless Internet service provider has an expense to install the client's premises equipment, which includes the cost of the equipment and the time of the technician to install and test the equipment. The wireless Internet service provider must recover this cost, which can be done with one of two methods.

- Charge the customer for the installation before proceeding with the installation.
- Amortize the cost of the installation with the customer's monthly payments for the service.

The first option is preferred by the wireless Internet service provider, but may cause the prospective customer to decide not to install the service due to the initial cost of the installation.

The second option is more attractive to customers as each monthly payment will be small when compared to the cost of the installation. The wireless Internet service provider has to ensure that the customer maintains the service for a minimum period of time in order to recover the cost of installation and not loose money. It is necessary to have a written agreement between the wireless Internet service provider and the customer specifying the terms and conditions.

- The customer must commit to using the service for a minimum period, which can be one year or two years. The wireless Internet service provider should plan to amortize the installation cost within half the minimum contract period.
- If the customer desires to terminate the agreement early then the customer must pay a termination fee so that the wireless Internet service provider can recover the cost of the installation.

The wireless Internet service provider should consult a lawyer to prepare an agreement that incorporates all aspects of local laws. Most lawyers will have access to a pre-prepared agreement that needs only specific alterations for the providers business.

2.6. Mobile broadband Internet service

A mobile broadband service is provided in public areas and by businesses that offer services for the public. Some examples of mobile broadband providers that charge for the service are listed below.

- WISP hotspot service for mobile devices.
- Airports.
- Internet cafes.
- RV parks and campgrounds.
- Marinas.

Some examples of free mobile broadband services, called WiFi Hotspots, are listed below.

- Restaurants, coffee bars, retail stores.
- Motels, hotels, and resorts.
- Municipal and state parks and campgrounds, municipal sports arenas.
- Sporting events, team games, sports clubs, and gymnasiums.
- Shopping malls.
- Churches, schools and colleges.
- Trade shows.

A mobile broadband installation is shown in the following figure.

Figure 2.6.1. A mobile broadband campground Hotspot installation with a PtMP wireless access point and a PtP backhaul antenna provides Internet for visitors and an on-demand charge is made for the service.

The mobile broadband customer can use any mobile wireless device, smart-phones, tablet or laptop, to connect to the PtMP wireless access point. The mobile broadband customer is anonymous to the broadband provider and pays for an Internet connection for a specific duration (pay-on-demand). An access code is purchased which allows the mobile broadband customer to login via the captive portal login screen or pay-wall. The customer remains connected for the duration specified by the code. The maximum distance that the mobile device can connect to the PtMP antenna is a few hundred meters. The mobile broadband customer has rate-plan conditions imposed on the service provided. The rate-plan conditions can include the maximum download and upload speeds permitted, and/or the maximum download and upload byte count permitted.

In some cases the mobile broadband service is provided without charge, as this is part of the services offered by the public or business entity. All hotels and motels offer free Internet when advertising for customers. Other mobile broadband Internet providers charge a fee for use; this is the case with many airports, especially International airports. There are situations where the mobile broadband service is both free and paid. One example of this is hotels where free WiFi is offered to hotel guests at a slow download and upload speed. If the hotel guest wants faster download and upload speeds then the guest can purchase the fast service using a credit card.

An important characteristic of the mobile broadband service is that the wireless access point WiFi antenna has no encryption, unlike a wireless access point installed in a business or installed for fixed broadband use, where the data connection will be encoded using WPA2 or WPA2-enterprise encryption. When the transmission is encrypted the credential is maintained as a secret and known only to the technical people who installed the network. Encryption protects the wireless network from hackers. In the case of mobile broadband there is no purpose in having encryption because the encryption key must be given to everyone, eliminating the security value of a secret key. The users can encrypt individual transmissions by connecting to a website using encryption (HTTPS://) or else installing reliable VPN software before using a mobile broadband service.

Mobile broadband is a very popular form of providing Internet access in developing economies for two reasons.

- People use mobile phone WiFi to access the Internet and will connect to unencrypted public WiFi Hotspots.
- Some people prefer on-demand payment in preference to paying a subscription, which means that they purchase an access code for a limited duration when they want Internet access.

Mobile broadband products that issue access codes to customers based on the Hotspots scripts for Mikrotik wireless access points have a limitation that the access code will only work with the wireless access point for which it was issued. Mobile broadband customers want to move between different wireless access points that are part of the providers network, either when the wireless access points are at the same location, or at different locations.

Mobile broadband that permits movement between multiple wireless access points can have one of two types of operation.

- Mobility. The customer receives an access code and can move between different wireless access points in the same network, however the customer must repeat the login process at each wireless access point.
- Roaming. The customer receives an access code and can move between different wireless access points in the same network, when the customer has logged in to the first wireless access point then the customer remains connected to the Internet at any other wireless access point, there is no need to login at each wireless access point.

Mobility and roaming is implemented by one of two means.

- Install many wireless access points, which are wired back to one access control router to authenticate the customer's access code. Access codes issued by the central access control will work with any one of the wireless access points connected to it. The wireless access point might be connected back to one central access control router location in a small town using point-to-point wireless connections, or on a larger scale might be connected back to a central access control router location through a VPN configuration. The central access control router can support both mobility and roaming.
- Install wireless access points that each have access control software, and authenticate access codes by communicating with a cloud management system that provides access code authentication and supports both mobility and roaming.

Mobile broadband roaming works in a similar manner to the mobile phone network. The customer connects to one wireless access point and is authenticated using the access code that was purchased from the WISP. The customer can then move to a different wireless access point location and remain connected to the Internet without a second login. The customer can move between wireless access points until the duration of the code expires. Popular mobile broadband wireless and access control products rely on cloud management to centrally generate and authenticate access codes while the access control of users occurs at the wireless access point, to implement both mobility and roaming.

The PtMP tower infrastructure can be used for both fixed broadband and mobile broadband customers when the PtMP wireless is configured with two broadcast channels, called Service Set Identifiers (SSID's). One SSID will be encrypted for fixed broadband customers using WPA2 or WPA2-enterprise, while the second SSID that provides access for mobile broadband customers is not encrypted.

In addition to implementing mobility with roaming, cloud management can also provide other valuable functions such as monitoring the status of each wireless access point, and generating an alarm if any wireless access point fails or goes off-line. Some cloud management services have a monthly or annual charge for use with popular routers and wireless access points such as those manufactured by Mikrotik. Other cloud services are provided free of charge by product manufacturers for use exclusively with their products.

A mobile Internet service provider can partner with one of the global mobile WiFi subscription companies to provide the service is provided at a busy location such as an airport. The Internet service provider will invest in the installation of wireless access points and share the revenue in exchange for the brand marketing and subscription customers of the WiFi service. Although this type of partnership can bring results for locations such as airports where the global brand is familiar, it is not beneficial to a city network in a country where the brand does not advertise.

The following diagram illustrates the cloud management of several wireless access point antennas. The customer can connect to any antenna with one access code and move to a different antenna and remain connected to the Internet through the automatic authentication process of the cloud roaming service.

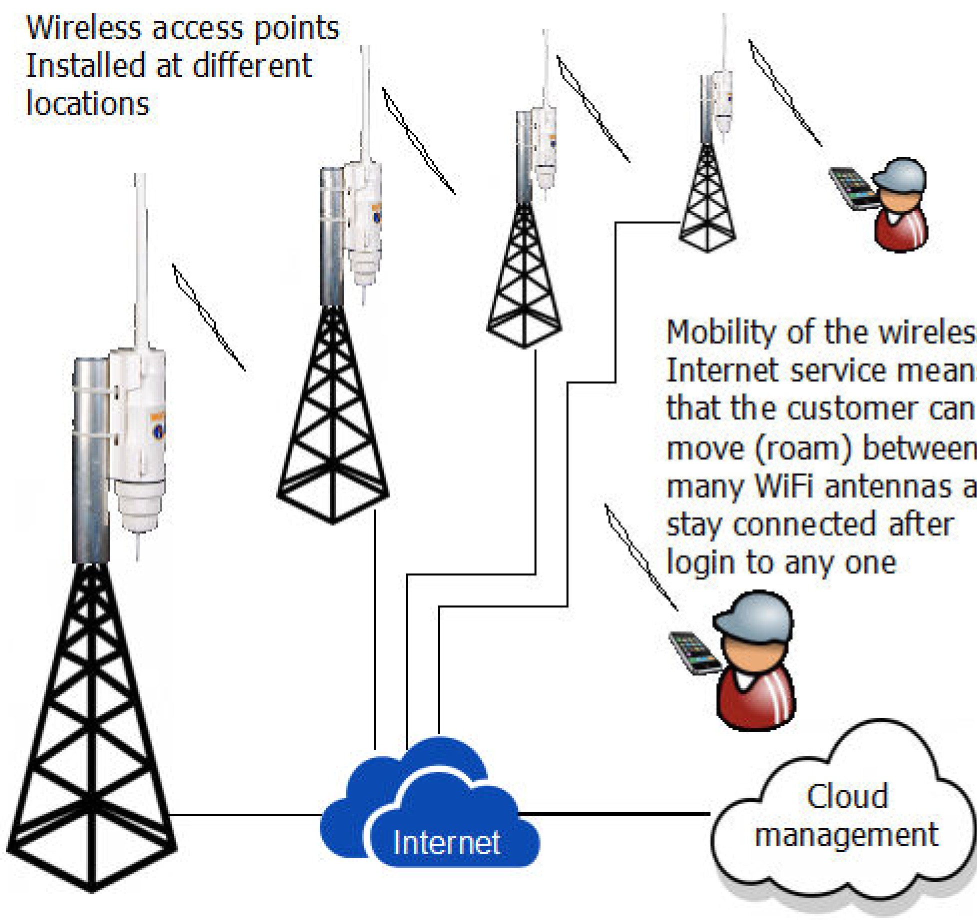


Figure 2.6.2. Mobile Broadband service with roaming where a customer logs in to one wireless access point and remains logged in when accessing other wireless access points that are part of the same network.

With mobility and roaming technology the wireless Internet service provider can offer a mobile broadband service with coverage of a village or town. PtMP wireless access points are placed at high points such as the roofs of buildings so that customer mobile devices have good visibility of the PtMP antennas. The mobile broadband Internet service provider can print access code vouchers at a central location then distribute them throughout the city to be sold at many retail points. A customer can then purchase access anywhere in the town and then connect to the Internet at any point in the town. The customer can move around using one access code purchase to connect to the Internet at any location of the network.

2.7. Locating and using the wireless access point

The WISP's customer can connect a computer, tablet or smart-phone to a point to multi-point (PtMP) wireless access point antenna either directly (mobile broadband) or via a CPE installed at the customers premises (fixed broadband). A number of subscribers can connect to the PtMP antenna simultaneously. The WISP PtMP wireless access point is installed outdoors at a high point, on a mast or the roof of a building. The subscriber must have a line-of-sight to the PtMP antenna as the wireless signal cannot pass through buildings or trees, therefore that the higher the antenna can be installed, then more potential customers will have access to the antenna. The figure shows the principle of the PtMP wireless access point and access control router.

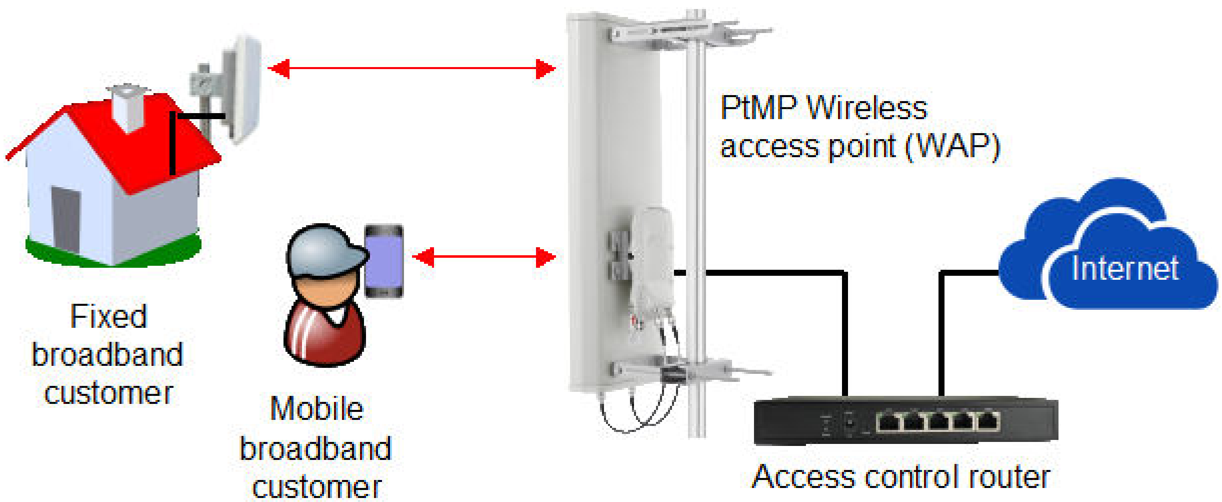


Figure 2.7.1. Point-to-multipoint (PtMP) wireless access point.

The WISP can provide a service for both the Hotspot customer who is a casual mobile broadband user and is paying for the on-demand for the service, and for the fixed broadband subscriber who has an agreement with the WISP to receive the Internet service and pay monthly for that service. The PtMP tower infrastructure can be used for both fixed broadband and mobile broadband wireless customers when the PtMP wireless is configured with two broadcast channels, called Service Set Identifiers (SSID's). One SSID will be encrypted for fixed broadband customers using WPA2 or WPA2-enterprise, while the second SSID is not encrypted and is used by mobile broadband customers.

The primary WISP customer is the fixed broadband subscriber. This customer will subscribe or sign up for the WISP service for a specific duration, usually 1 year. The WISP will install a client wireless device at the subscribers premises in order to connect with the WISP PtMP antenna over a long distance, up to a few Km. The WISP may charge the client for the wireless installation, in which case the client may or may not own the wireless device, or the WISP may charge an additional monthly fee for the rental of the equipment. The wireless link between the client wireless device and the

PtMP antenna is encrypted to prevent a third party trying to hack into the WISP's network connection. The WISP can authenticate the client wireless device (CPE) onto the network as this device is associated with that customer.

The mobile broadband Hotspot client is anonymous and will either purchase a means of access to the Internet via a cash payment for a voucher with an access code, or else pay online with a credit card to get Internet access. The mobile broadband Hotspot client can be a traveler in an airport or hotel, or a sports fan in a stadium. The range of the Hotspot PtMP antenna is limited because the customer's mobile device has a limited range and can communicate only up to a few hundred meters. The PtMP wireless access point for the Hotspot application is configured without encryption so that any person within range of the antenna can connect to it. Unfortunately with all Hotspots it is easy to hack the clients wireless connection, unless the client is connected to an encrypted server (HTTPS://). Access control for mobile broadband is implemented using a login or splash page. The mobile broadband Hotspot customer is a special case for the WISP. WISPs may be asked to provide a Hotspot service by a business customer, such as a hotel or conference center. The business arrangement can be made with the business customer or directly with the Hotspot users.

The PtMP antenna must be visible to the subscriber. Trees and buildings block the frequencies used for transmission (2.4GHz and 5.8GHz). When the antenna is mounted at a high point then more potential subscribers will have visibility to the antenna. There are three popular locations to install a PtMP antenna;

- On top of a tall building.
- On a tower designed for mounting antennas.
- On a hilltop that overlooks the area of coverage.

A tall building is a good location for an antenna. The building will be located in the area where the WISP wants to sell the Internet service. In addition a building will have power and it may be possible to contract an Internet service, such as fiber or copper data cable at the building. The WISP should contact the building owner or manager, and if the antenna installation is permitted then a monthly fee will be paid for the antenna location. Wireless phone operators prefer to install mobile phone antennas on tall buildings when possible. Mobile phone companies are willing to pay a high sum of money to the building owner for use of the location. If the building owner asks the WISP to pay a similar quantity of money that a mobile phone company pays then the cost will not make economic sense for the WISP business.

An existing antenna tower that already has mobile phone antennas is a good location to install the WISP antenna, as it will have power and Internet access. The tower owners however are accustomed to receiving payments from mobile phone companies and the values they pay are much too high for a WISP business. There are some tower owners however who understand the economics of the WISP business and are prepared to accept a much lower fee for the installation of a WISP antenna. The WISP should always approach a tower owner and try to negotiate. The installation of an antenna on the tower requires the expertise of a person skilled with tower installations. In the USA a tower climber will have to be certified, licensed and insured in order that the tower owner will permit the installation. Most likely a tower owner has installation contractors to install antennas. Laws about antenna installations vary between countries.

A hilltop is a convent location to install an antenna if the terrain has a hill overlooking the area of coverage. If a hilltop is the best location to install an antenna the WISP must negotiate with the person or business that owns the land to install equipment at the site. If an antenna installation is permitted then the landowner will request a rental fee for use of the location. If the PtMP antenna is installed on a hilltop then the Internet backhaul will be a wireless point-to-point (PtP) connection to the NOC. The location will require a solar and wind energy system to power it. These topics are covered in later sections.

A final alternative for the WISP is to purchase and install a tower. The WISP will need to purchase or rent a small piece of land, and purchase an antenna tower for installation on the land. The cost of an antenna tower is not high however the installation of the tower will cost more. A civil engineer will be required to calculate the foundation required and a considerable amount of steel and concrete will be buried in the ground to support the tower. Local governments will also require a licensed construction professional to pull permits for the installation, and will inspect the work to ensure that it meets the relevant construction codes. Retractable towers are also available installed on trailers, which can be towed to the location where the antenna will be installed. The trailer tower does not require a foundation because the trailer is equipped with retractable legs, which will spread the antenna load over a large area for stability. Taller antenna towers may require anchoring wires for stabilization, and each of the wires will need a foundation and will require a larger area around the tower site.

Always consult an antenna tower professional when considering the option of installing an antenna tower as mistakes can cause a lot of damage and be expensive to correct.

The startup WISP should seek either a hilltop location to install the antenna, or else find a tall building where the owner will charge a small fee for the antenna installation. Antenna towers are usually a larger expense and should be considered when the WISP business is making money and can afford the expertise required for the installation.

2.8. Wireless access points and antennas

When making a decision about the purchase of a wireless access point for the PtMP installation, the most important considerations are the antenna gain and the antenna radiation pattern. The antenna determines the quality and propagation distance of the wireless signal, which directly corresponds to the number of prospective subscribers who will be able to connect to the antenna.

There are two categories of antenna radiation patterns, directional and omni-directional. Often new WISP’s install a PtMP radio with an omni-directional antenna, however this is the worst type of antenna for WISP applications. An omni-directional antenna is excellent for a ship to shore VHF radio as both the ship and shore antennas will be at the same height, and the ship turns on a circular axis. For WISP applications a directional antenna will give much better results when used as a PtMP antenna. Mobile phone towers always have directional antennas installed and a WISP installation is very similar to the mobile phone wireless installation.

Antennas also have a characteristic called gain, which is measured in decibels (dB). Antenna gain is not the same as amplifier gain. An amplifier uses an electronic circuit to increase the voltage of an audio or radio frequency (RF) signal. The amplification factor is called gain and is measured in dB. Antenna gain does not mean that the signal is amplified, it means that the antenna is pointing the RF energy in a specific direction and so the gain is the difference in RF signal strength between the direction that the antenna is pointing and the direction it is not pointing. The antenna gain is part of the calculation of the transmission power, called effective radiated power (ERP), which determines the range of the antenna. The ERP is calculated by summing the radio amplifier output in +dBm with the antenna gain in dBi. In the USA ERP must not exceed +36dBm. In other countries the WISP should consult local regulations regarding the maximum permitted antenna transmission power.

WISPs obtain two advantages by installing directional antennas for PtMP wireless applications.

- A directional antenna radiation pattern can be selected to cover the area where the prospective subscribers are located.
- The directional antenna can communicate over a much longer distance in the direction that the energy is focused.

Antennas also have a characteristic called polarization, which can be vertical, horizontal, circular clockwise, circular anti-clockwise or a combination of polarizations. The polarization of the transmitting and receiving antenna should be the same. Most antennas in use at the present time are multiple-input and multiple-output, (MIMO) which means that the antenna can multiply the capacity of a radio link using multiple transmission and receiving antennas for multi-path propagation. MIMO antennas are installed with popular data communications methods, including IEEE 802.11n (WiFi), 802.11ac (WiFi), WiMAX, and Long Term Evolution (4G LTE). Five popular antenna types are explained in the following sections, two are omni-directional and three are directional.

Omni-directional antenna: The omni-directional antenna is very common for VHF radio applications like a VHF 2-way radio installed on a boat. The omni-directional antenna is the least desirable type of antenna for WISP applications because the RF propagation characteristics give poor results for PtMP applications. The RF propagation characteristics are illustrated in the figures that follow.

The RF radiation maximum strength is perpendicular to the antenna. The propagation area of the antenna is measured at the signal strength -3dB points. The -3dB points indicate where in space the RF power is reduced to half, the dB (decibel) scale is logarithmic. The RF radiation intensity can be represented by a 'doughnut' around the antenna as shown in the next figure, with the area of maximum RF energy at the horizon. The gain of the antenna determines the angle between the upper and lower -3dB points; the higher the gain the smaller the angle.

The effectiveness of the omni-directional antenna can be viewed using the radiation profile diagram in the figure. At ground level obstacles block the RF radiation emitted by the antenna. Dense objects absorb the radio frequencies that are used for license-free data communications of 2.4GHz and 5.8GHz. When the omni-directional antenna is used for VHF applications then the RF radiation is not greatly attenuated by obstacles due to the longer wavelength.

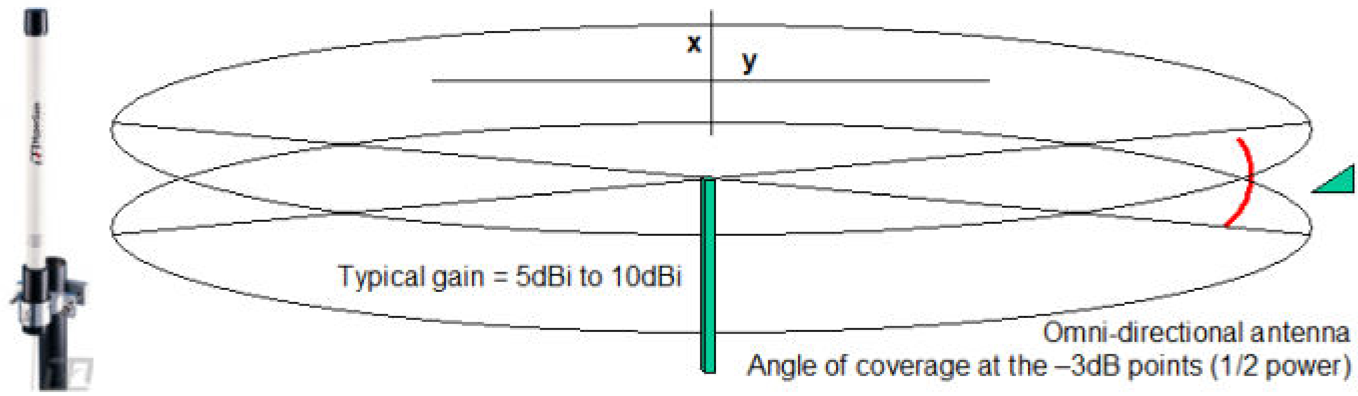


Figure 2.8.1. Omni-directional antenna RF radiation pattern.

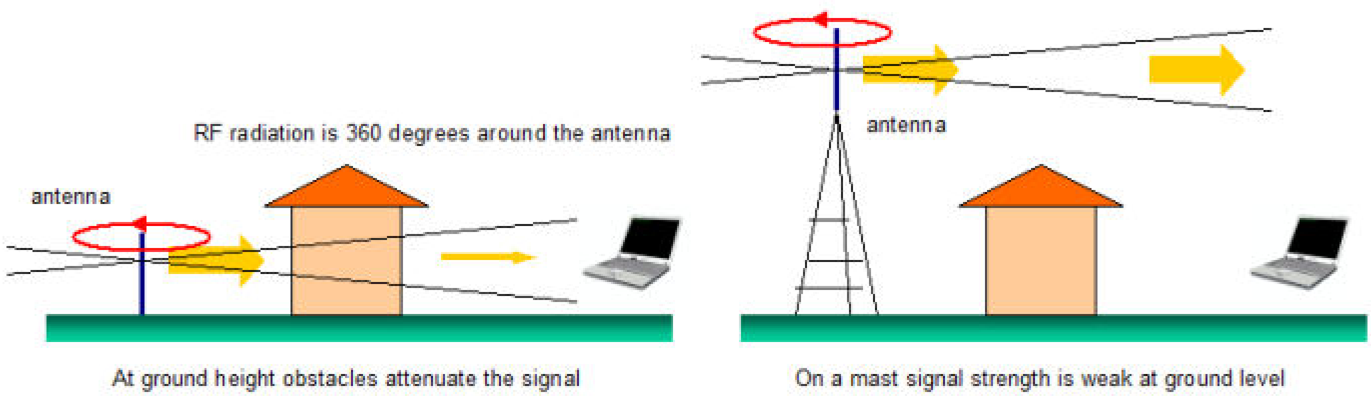


Figure 2.8.2. Omni-directional antenna RF radiation profile.

The WISP can have a good visualization of the omni-directional area of coverage by superimposing the energy density onto a photograph of terrain. This is shown in the next figure. It is clear from the diagrams that the maximum energy density is directed above the area where the prospective subscribers are located. RF energy is radiated 360 degrees around the antenna and as RF energy may be covering areas with no customers then the antenna is wasting energy. A directional antenna is much more efficient as RF energy can be pointed to the area with residents. The omni-directional antenna with corresponding wireless access point is more expensive then some alternative antenna configurations.

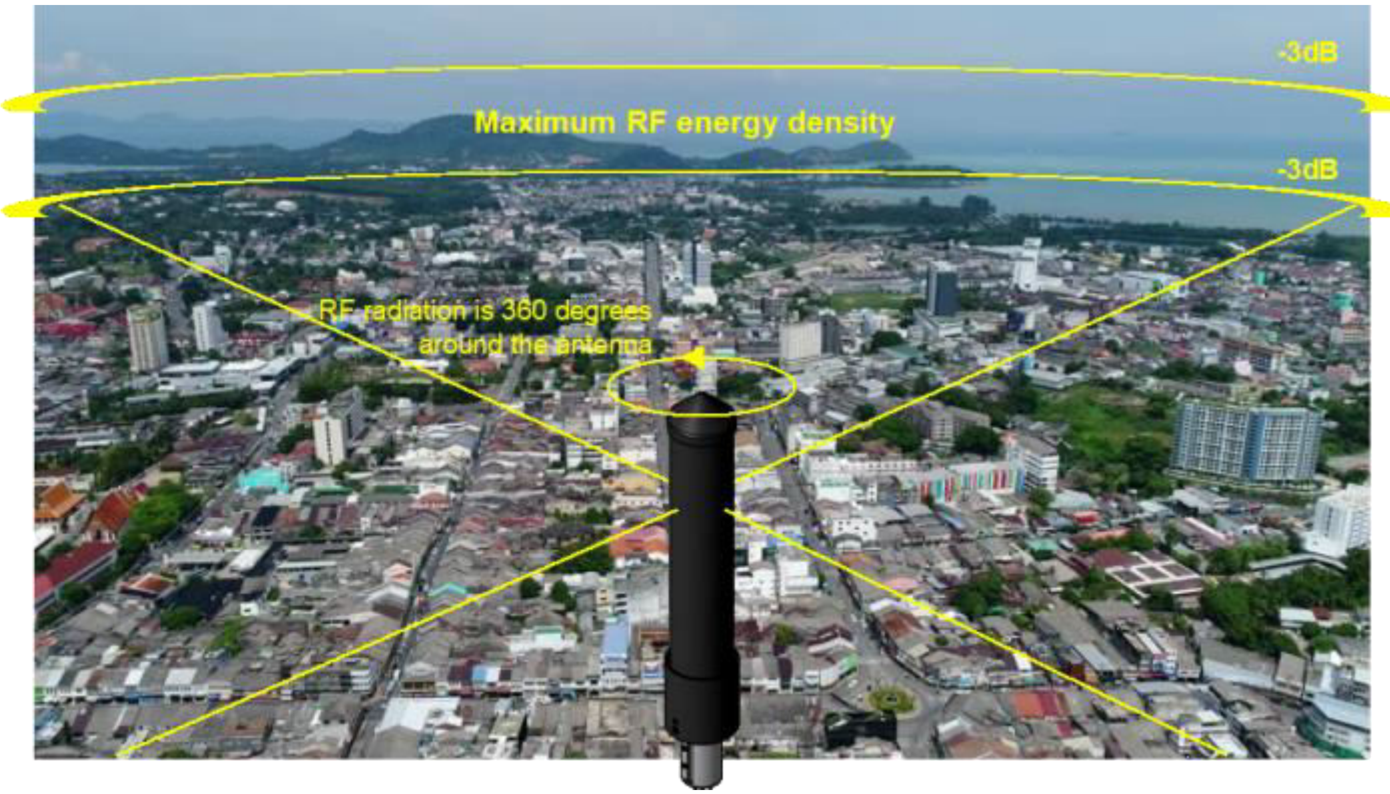


Figure 2.8.3. Omni-directional antenna radiation field strength.

Omni-directional antenna with down-tilt: The down-tilt omni-directional antenna is designed to overcome the primary failing for the omni-directional antenna for PtMP applications. The RF radiation is tilted down so that the area of high RF energy density is a region on the ground instead of the horizon. The down-tilt omni-directional antenna was designed as a solution for PtMP applications however the antenna has two limitations;

- The antenna direction cannot be adjusted and so the antenna cannot be pointed towards the area of maximum subscriber density.
- The energy is radiated 360 degrees around the antenna and energy is wasted if prospective subscribers are not located 360 degrees around the antenna.

The propagation characteristics of the down-tilt omni-directional antenna are illustrated in the next figure. The effectiveness of the down-tilt omni-directional antenna can be viewed using the radiation profile diagram in the figure that follows. The radio frequency energy is directed towards the ground, and with some antennas the antenna down tilt angle can be adjusted electrically.

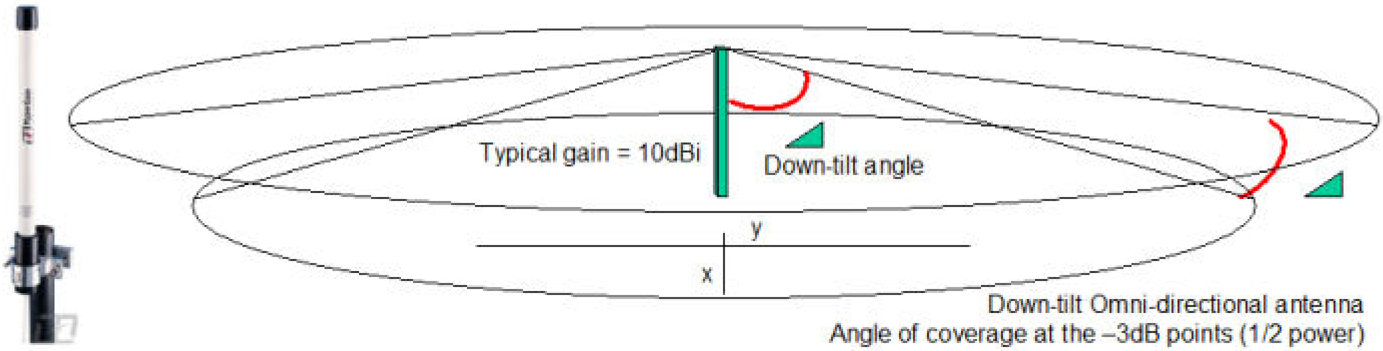


Figure 2.8.4. Down-tilt omni-directional antenna RF radiation pattern.

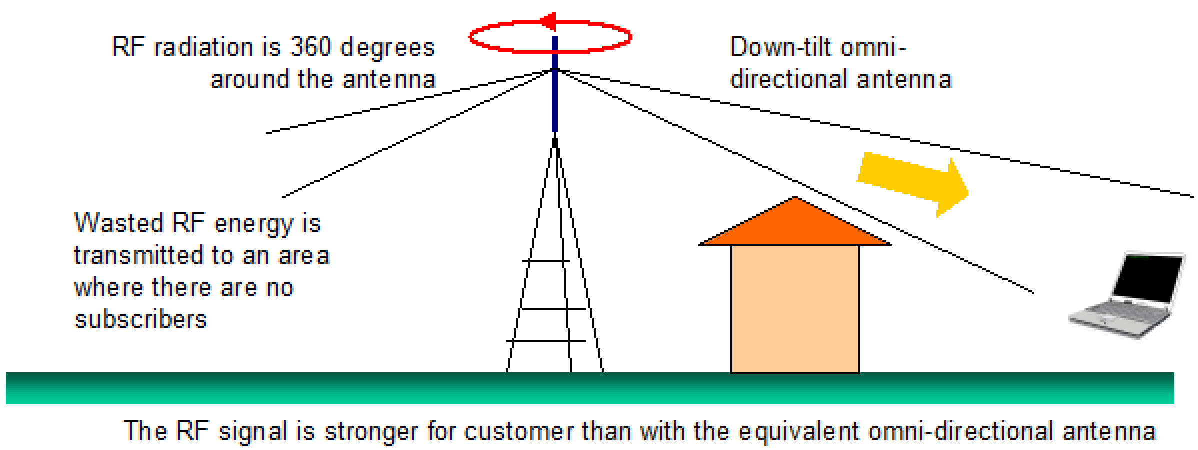


Figure 2.8.5. Down-tilt omni-directional antenna RF radiation profile.

The following figure provides visualization of the down-tilt omni-directional area of coverage by superimposing the energy density onto a photograph of terrain. Compared with the omni-directional antenna, the area of maximum RF density has been moved down from the horizon to part of the area where prospective subscribers may be located.

The RF energy is radiated 360 degrees around the down-tilt omni-directional antenna and so RF energy will be directed to areas where no subscribers are located. Once again a directional antenna will be more efficient as RF energy can be pointed to the area with high customer density. The down-tilt omni-directional antenna costs more than the omni-directional antenna. The installation is also more expensive as there are no down-tilt antennas with integrated wireless so these items are purchased separately then connected with an RF cable.

Figure 2.8.6. Down-tilt omni-directional antenna radiation field strength.

Directional panel antenna: The panel antenna is a good choice for a WISP application. It is not the most efficient antenna, however a panel antenna installation will cost less than any other antenna installation because many PtMP wireless access points have integrated panel antennas. The 2.4GHz integrated wireless and antenna products are very low cost as they are manufactured in very large volume. The panel antenna is directional and the propagation pattern is usually rectangular. Horizontally the antenna radiation may cover 60 degrees of arc, while the vertical coverage might be 30 degrees of arc. The RF radiation pattern is shown in the next figure.

When the panel antenna is mounted on a mast it can be pointed downwards towards the area where the potential subscribers are located. When the antenna is mounted on a high point then subscribers have a clear line-of-sight to the antenna, which is necessary to establish a wireless connection.

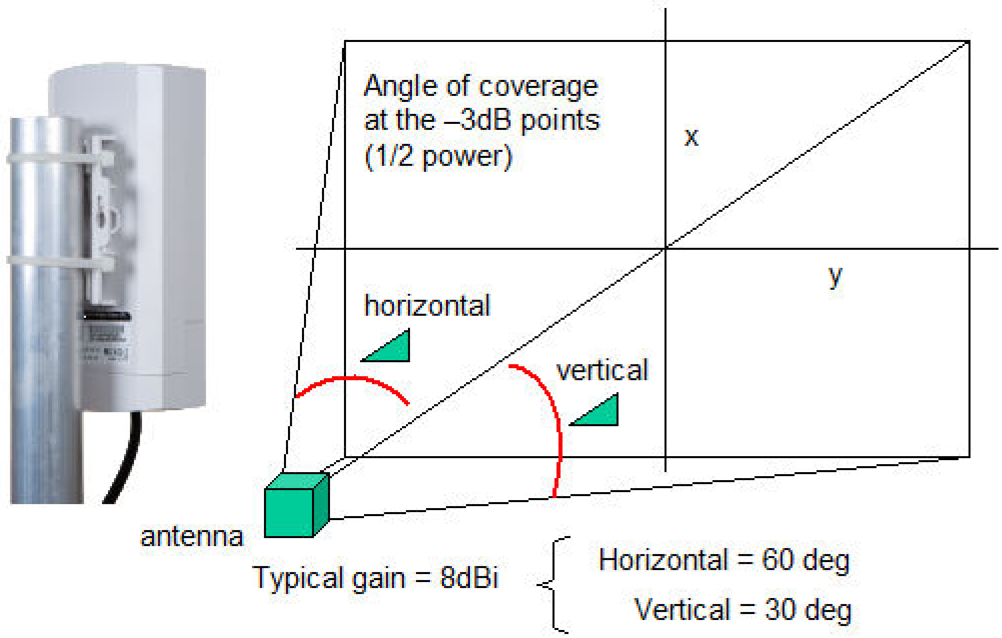


Figure 2.8.7. Panel antenna RF radiation pattern.

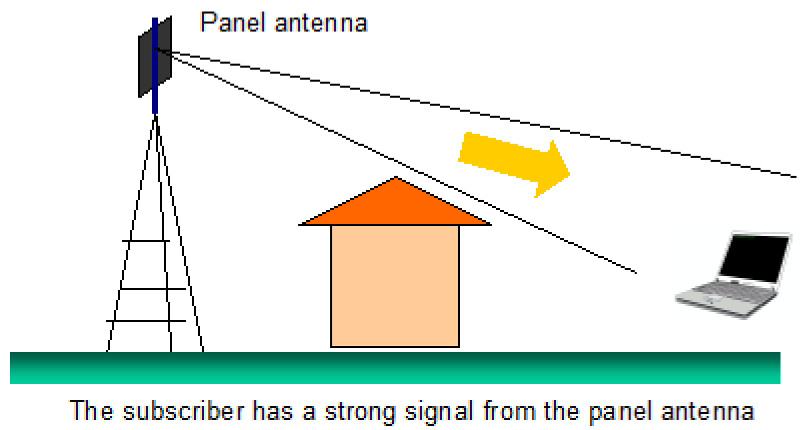


Figure 2.8.8. Panel antenna RF radiation profile.

The panel antenna coverage area can be visualized by superimposing the antenna radiation signal strength pattern onto a photograph of terrain, as shown in the next figure. The panel antenna offers good flexibility to adjust the area of coverage by attaching it to a mast with a mounting that can be tilted up and down, and side to side. Because the panel antenna has been integrated with the wireless electronics then installation is much easier and lower cost than alternative antenna solutions.

Figure 2.8.9. Panel directional antenna radiation field strength.

If the arc of coverage desired is larger than that of a single antenna then several panel antennas can be mounted around a mast. Using an antenna that has a horizontal arc of coverage of 60 degrees, six antennas can be mounted around a tower to cover 360 degrees, as shown in the figure below. It is not common to provide 360 degrees of coverage, more likely the WISP will want to cover an arc of 180 degrees or less.

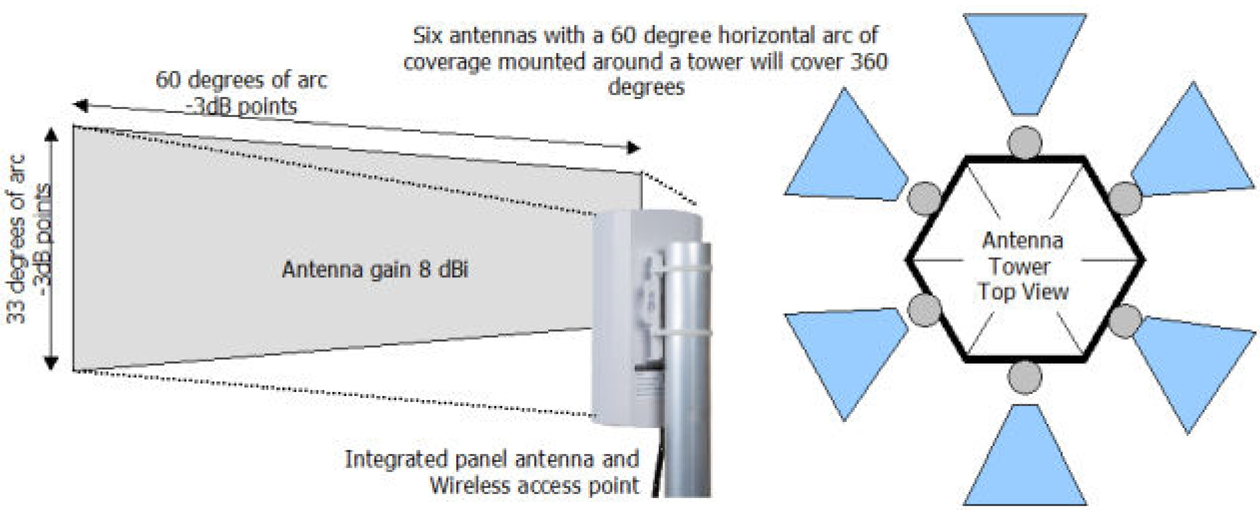


Figure 2.8.10. Panel antenna RF radiation for 360 degrees.

Directional sector antenna: The sector antenna has good propagation characteristic for PtMP wireless applications. Mobile phone PtMP communications towers use sector antennas exclusively. The sector antenna covers a fixed sector of arc, and is manufactured with 90 degrees, 120 degrees, and 180 degrees of arc. Coverage of 360 degrees around the tower can be obtained with four 90-degree sector antennas, three 120-degree sector antennas or two 180-degree sector antennas. The most common type of sector antenna installed onto mobile phone towers is the 120-degree antenna and mobile phone towers have three antennas installed to cover 360 degrees around the tower for urban installations. Although the sector antenna is technically the better solution it is also more expensive to manufacture and there are few integrated sector antennas with wireless access points. The antenna and wireless are purchased separately and RF cables are required to connect the two. 'Carrier-grade' PtMP installations will have sector antennas and robust wireless units. For unlicensed spectrum the high performance sector and wireless products will be dual band (2.4GHz and 5.8GHz) and offer a total throughput in the hundreds of Mb/s range.

In addition to the 90, 120 or 180-degree arc of coverage, the vertical arc is generally small, less than 10-degrees. Sector antennas are usually designed for high gain, ranging from 10 dBi to 20 dBi. The radiation pattern of a sector antenna is shown in the next figure.

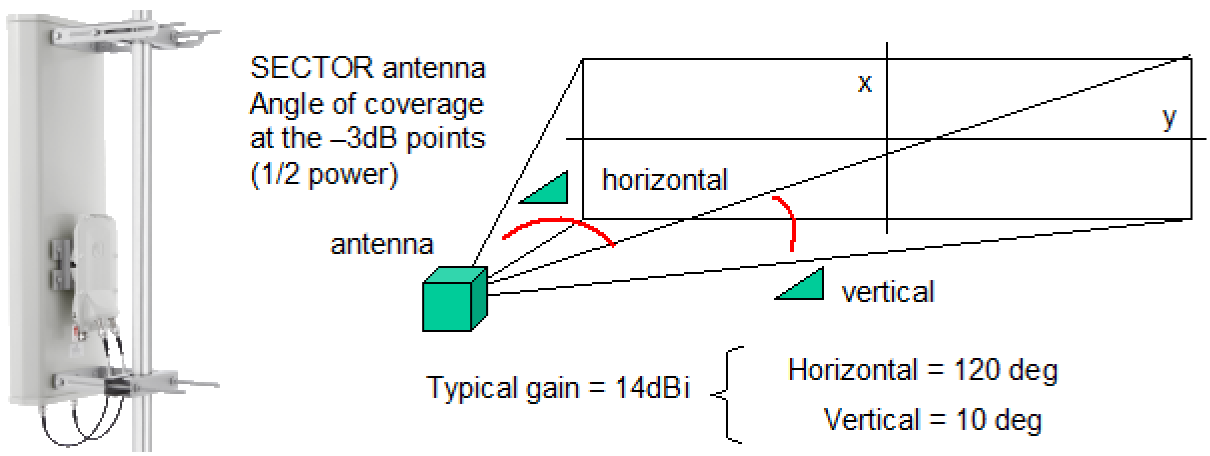


Figure 2.8.11. Sector antenna RF radiation pattern.

The radiation profile of the sector antenna is illustrated in the next figure. With the antenna mounted on a mast or high building the subscriber has direct line-of-sight to the antenna.

The estimated RF propagation area is superimposed onto a terrain photo to illustrate how the sector antenna can provide coverage for a larger area with better signal strength when compared with other antenna designs.

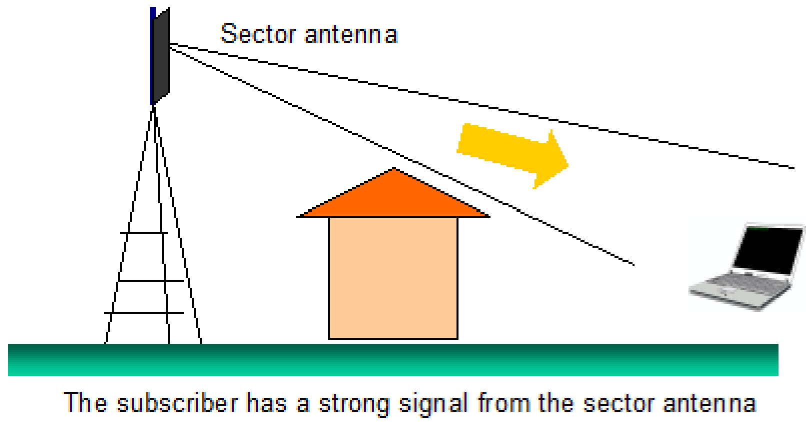


Figure 2.8.12. Sector antenna RF radiation profile.

Figure 2.8.13. Sector directional antenna radiation field strength.

The figure at the right shows the installation of three sector antennas on a communications tower in an urban area. Each sector antenna has a horizontal arc of coverage of 120 degrees, providing 360 degrees of coverage around the tower. A WISP installing a sector antenna on a tower may install more that one antenna to provide the arc of coverage for the location of the target customers. Sector antennas have a tilting adjustment that can tilt the antenna from horizontal to approximately 15 degrees below the horizon; the WISP will adjust the antenna vertical position tilt down to cover the desired area.

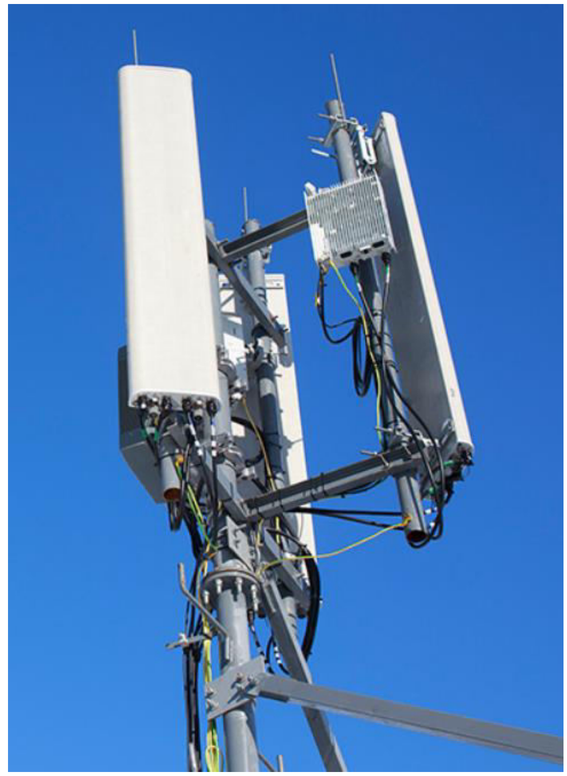


Figure 2.8.14. Three 120-degree sector antennas mounted on a tower.

Beam-forming directional phase-array antenna: The beam-forming antenna (sometimes called an adaptive array or smart antenna) offers the best propagation characteristic of the antennas available for WISP's. The phase-array antenna has many small antennas and each can have the phase of the radio frequency changed electronically. The antenna controller can modify multiple antenna phases in order to focus the beam in a specific direction.

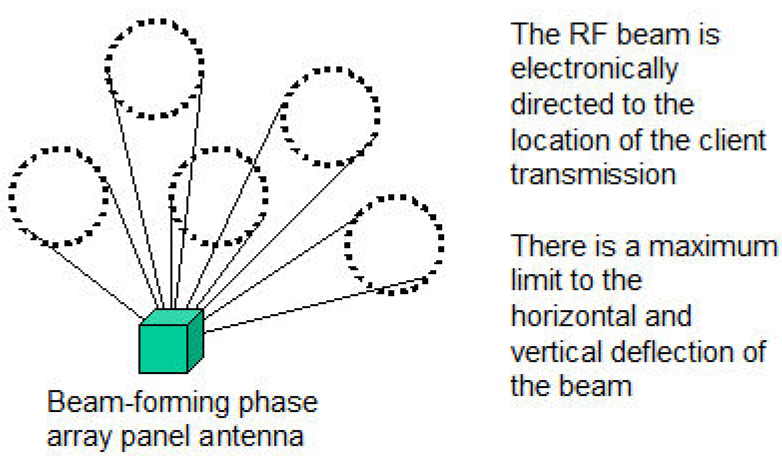


Figure 2.8.15. Beam-forming antenna RF radiation profile.

The direction of focus is limited to 180 degrees or less around the face of the antenna. When the antenna receives an RF signal from a client the direction of the signal can be measured and then the corresponding transmission from the antenna is focused in the direction of the client that transmitted the signal. Multiple clients can have connections to the antenna as the beam direction is switched in microseconds. The beam-forming antenna is the most expensive of the antennas described in this section as it requires additional electronics to adjust the direction of the beam.

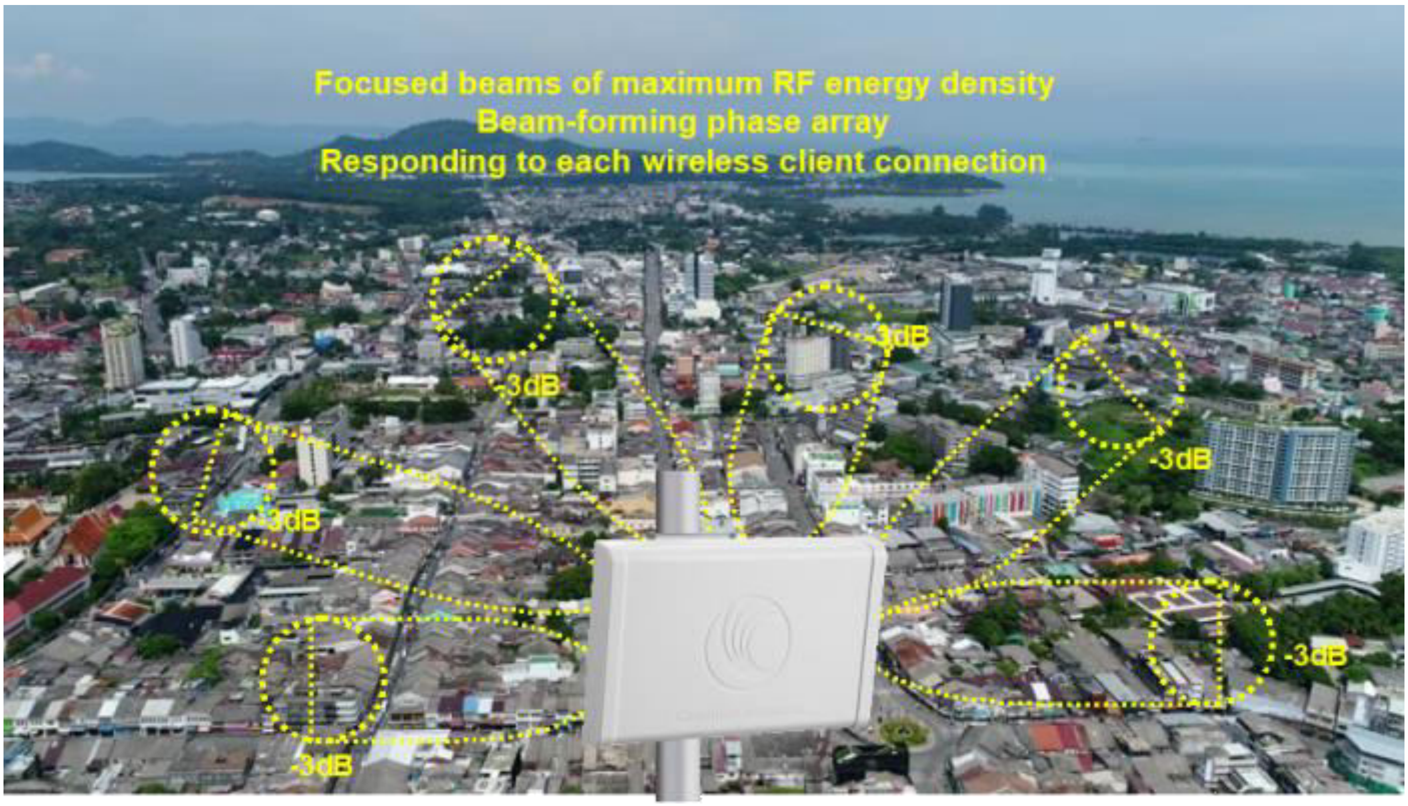


Figure 2.8.16. Beam-forming antenna radiation field strength.

Multiple PtMP antenna interference: Installing multiple PtMP wireless access point antennas on a tower can lead to interference between the antennas. When the WISP is installing multiple PtMP wireless access points ensure the each antenna has a non-overlapping frequency to minimize interference. The 5GHz band has a much larger frequency range available than the 2.4HHz band and 5GHz band is preferred for multi-antenna installations, although the equipment has a slightly higher cost.

Some PtMP wireless access point manufacturers add a GPS radio receiver to the access point. This permits the wireless access point transmission and reception of multiple PtMP units to be synchronized using the GPS signal, to avoid interference between multiple wireless access points preventing them from transmitting and receiving at the same time. GPS synchronization will improve the overall data throughput as the WISP expands to multiple PtMP antenna installations.

2.9. Client premise equipment and antennas

The fixed broadband customer can be located several Km from the Internet service provider PtMP antenna, providing that the customer has a line-of-sight view of the PtMP antenna. The long distance is possible because a wireless receiver with a high gain directional antenna is installed on the roof of the customer's premises. This wireless receiver with high gain directional antenna is called the Client Premise Equipment (CPE) as this was the name given to the product by telecom companies who connected the client last mile using wireless. The PtMP wireless access point is configured as a host, and the CPE wireless access point is configured as a client.

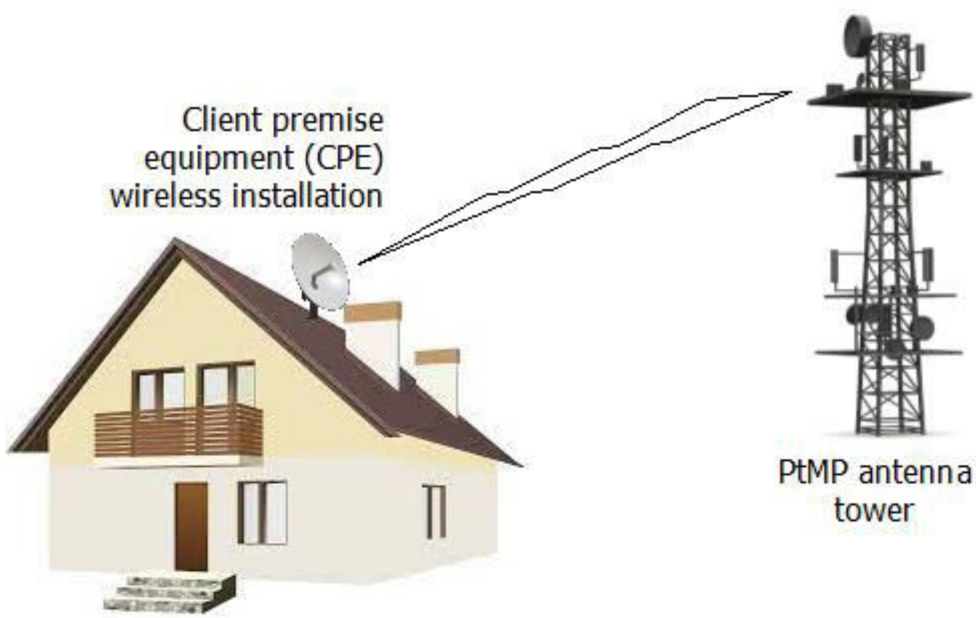


Figure 2.9.1. Installation of the client premise equipment antenna.

Some technical characteristics are listed below that are required to install the wireless directional antenna.

- The antenna must be installed securely at a high point on the building so that wind or other climate effects do not cause movement of the antenna.
- The antenna must have line-of-sight visibility to the transmitting antenna with clearance around the line-of-sight view (the Freznel zone, see the later section).
- The antenna position must be carefully adjusted for maximum signal strength using a signal strength meter incorporated into the CPE software.
- Outdoor Ethernet cable connects the CPE to the equipment inside the building. The Ethernet cable will carry the CPE data and also provide the CPE with power (Power over Ethernet).

The wireless Internet service provider is responsible for the installation of the CPE antenna on the roof of the customer's building. In addition to the CPE antenna the wireless Internet service provider must also install basic network infrastructure to permit the customer to connect any type of device to the Internet. Devices include wired desktop computers, and wireless laptop, tablet and smart-phone devices.

A typical residential client installation is illustrated in the figure below.

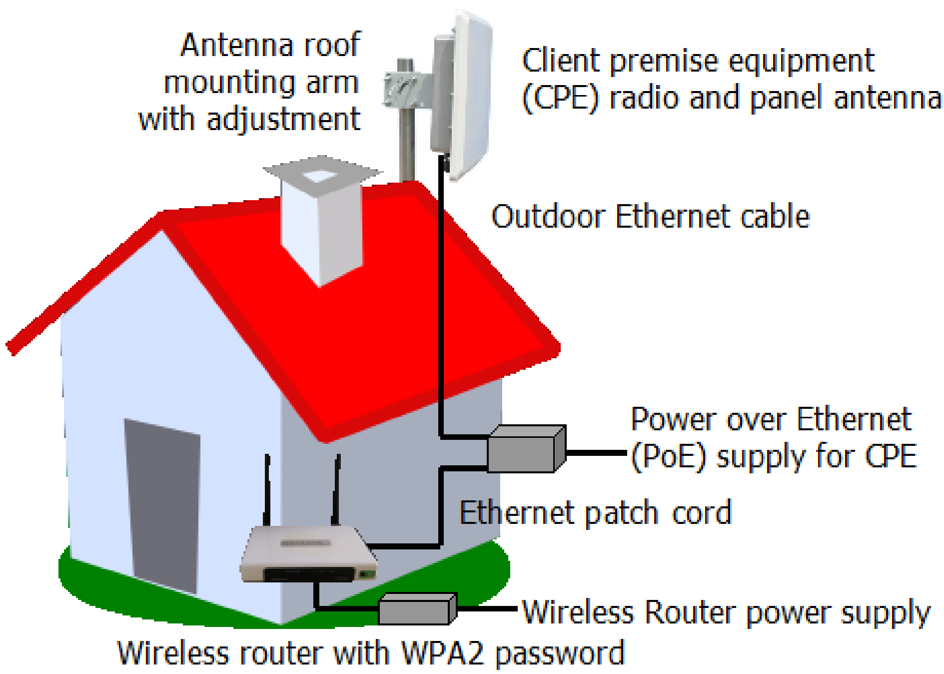


Figure 2.9.2. CPE installation in a residential building.

The wireless Internet service provider should prepare a customer installation kit which will include the following;

- CPE wireless and antenna.
- Adjustable roof mounting bracket for the CPE antenna.
- Outdoor Ethernet cable and connectors to connect the CPE wireless with equipment inside the building.
- Power over Ethernet power (PoE) supply to power the CPE wireless over the Ethernet cable.
- Wireless router with power supply providing Ethernet ports for several wired devices and WiFi wireless for several wireless devices.
- Ethernet panel cord to connect the wireless router to the PoE supply.

Two types of antenna are used in the CPE installation, panel and parabolic.

Panel antenna: the advantage of the panel antenna is simplicity and low cost. As the beam width is wide then the antenna is very easy to align with the remote PtMP antenna. The panel antenna has a medium gain with a distance of transmission of a few Km with line-of-sight. The following figures show a CPE panel antenna beam width and an antenna installed on a building roof.

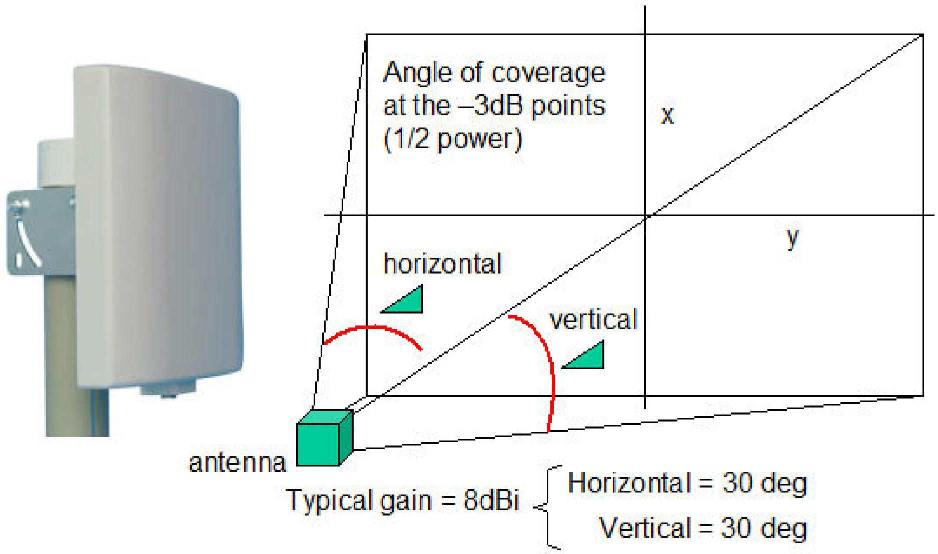


Figure 2.9.3. Panel antenna for a CPE installation.

Figure 2.9.4 CPE panel antenna installed on the roof of a subscriber building.

Parabolic antenna: Although the parabolic antenna is more expensive than the panel antenna it is preferred as the beam width is narrower with higher gain, and so the antenna can be located at a greater distance from the remote PtMP antenna. The narrow beam width means that adjustment of the antenna to focus onto the PtMP antenna requires patience to ensure good signal strength. The distance of transmission might exceed 10Km with good line-of-sight. The following figures show the typical beam width of a parabolic antenna, and show a parabolic antenna installed on the roof of a subscriber's building.

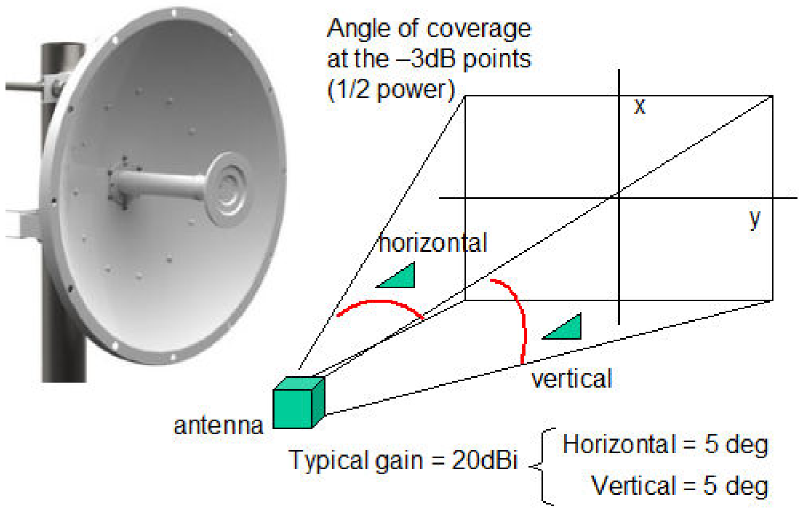


Figure 2.9.5. A parabolic antenna for a CPE installation.

Figure 2.9.6. CPE parabolic antenna installed on the roof of the subscriber's building.

When installing a CPE wireless choose the antenna based on the distance from the PtMP tower. Choose the patch antenna for shorter distances because it is easier to install and align. Choose the parabolic antenna for longer distances to get the maximum range from the PtMP antenna. Both antennas require line-of-sight. If the installation does not have line-of-sight to the PtMP antenna then it will be necessary to install a repeater or relay as some intermediate point where both the PtMP antenna and the CPE antenna have line-of-sight to the repeater.

2.10. Point-to-point wireless links and antennas

WISP network design has a connection point to the Internet at the Network Operations Center (NOC). The wholesale connection is a high capacity fiber or copper data circuit. The PtMP tower and the NOC may be several Km apart because the NOC has to be installed at a location where the wholesale network company can install the wholesale data circuit, and the PtMP tower has to be installed at a location that provides communications coverage for the maximum number of potential subscribers.

The WISP will install a point-to-point (PtP) wireless link between the NOC and the PtMP tower in order to provide the Internet connection at the PtMP tower. Each PtMP tower that the WISP constructs to expand the subscriber network will require a PtP wireless link from the tower to the NOC. The network of PtP wireless links between the towers and the NOC is called the Wireless Distribution Network (WDS). Wireless access points have an optional configuration called WDS enable, when the wireless device is used as part of the WDS. The WDS feature adds new data fields to the data packet so that the MAC address of the origin, which is the CPE device, can be passed to the destination, which is the NOC. The figure below illustrates the PtP wireless link between the PtMP tower and the NOC.

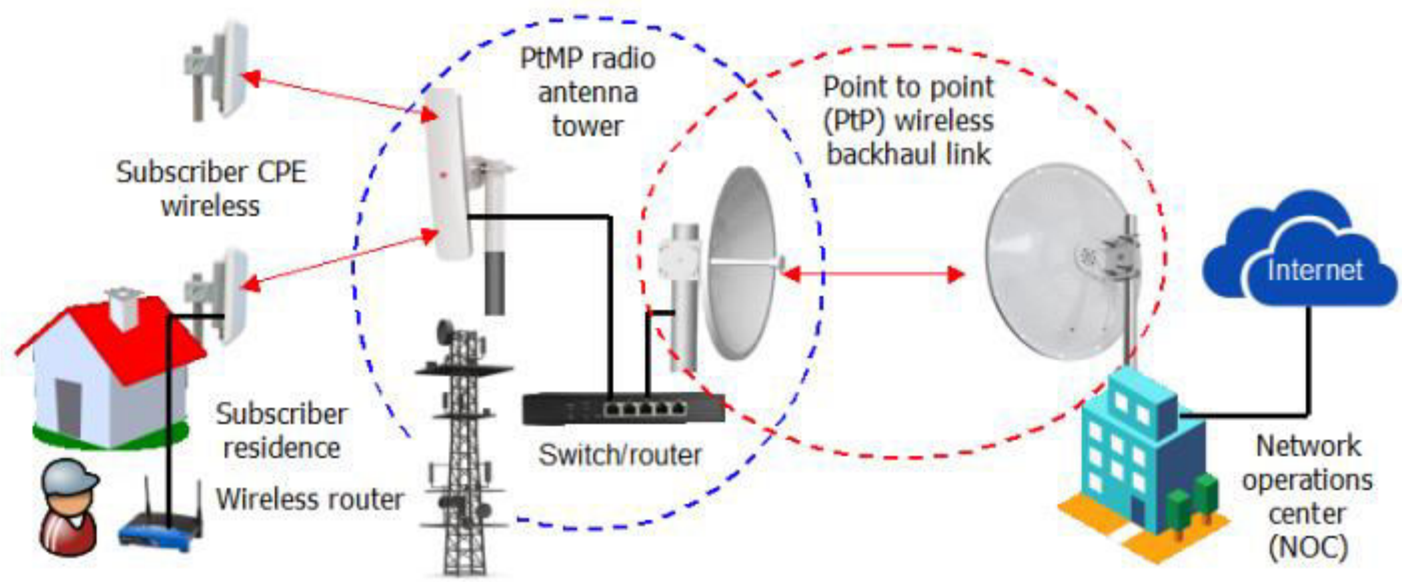


Figure 2.10.1. Point-to-point wireless backhaul link from the PtMP tower to the ISP network operations center (NOC).

As the line-of-sight PtP link has a maximum communications distance then if the tower is located further away from the NOC than the maximum distance a relay or repeater has to be installed in the path between the tower and the NOC to extend the transmission distance. If there is no line-of-sight between the PtMP tower and the NOC then an intermediate relay or repeater has to be installed in the path at a location where both the PtMP tower and the NOC have line-of-sight to the repeater.

The frequency band of 5GHz is popular for point-to-point links as there is less interference in this band, and many low-cost equipment options are available that offer very good data throughput performance. Data throughput is very important between the PtMP tower and the network operations center because this determines how many subscribers can connect to the PtMP tower.

In order to obtain the maximum distance of transmission over the PtP link the highest gain antenna is installed, which is the parabolic antenna. The parabolic antenna has a very narrow beam width that requires precision for alignment of the antennas. The wireless unit software has signal strength measuring features to assist with adjustments.

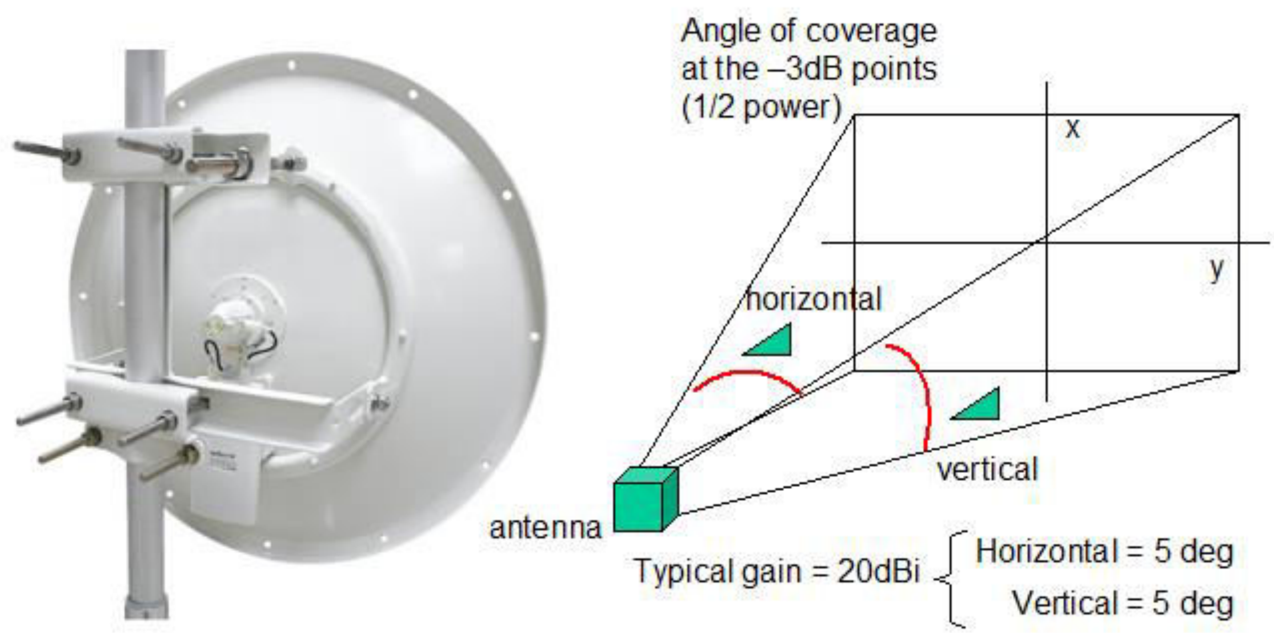


Figure 2.10.2. The 5GHz band wireless access point with parabolic antenna is popular for point-to-point wireless links.

Low cost point-to-point wireless equipment is designed for the 5GHz frequency band. The data throughput of the current equipment technology can be in the hundreds of Gbits/second due to the large bandwidth available in the 5GHz band. If higher data rates are required then point-to-point links for the 24GHz or 61GHz unlicensed frequency bands can be installed. Some manufacturers also make equipment for the 11GHz frequency band however this band is not available in all countries. The equipment for these bands can transmit at data speeds in the Gbit/second range, although at shorter distances than with the 5GHz equipment. The following figures illustrate 24GHz and 61GHz point-to-point antennas.

Figure 2.10.3. Full duplex wireless access point with antenna for the 24GHz unlicensed band (airFiber 24HD © Ubiquiti). The maximum transmission distance is 30Km.

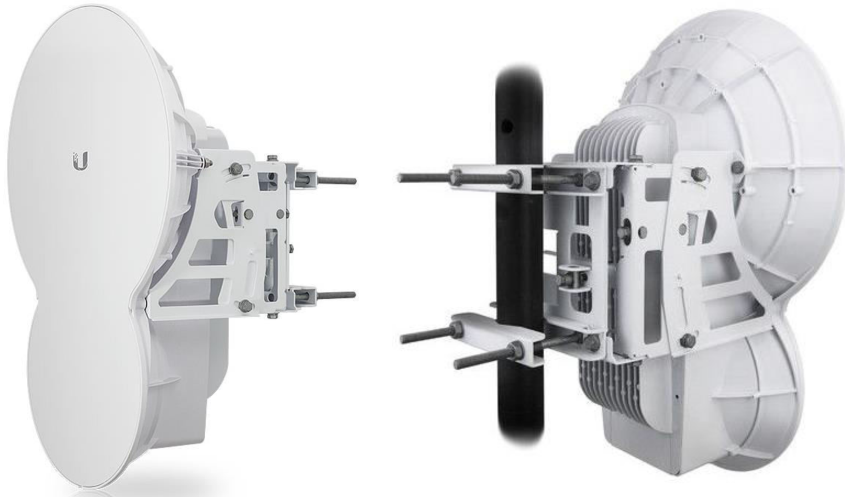


Figure 2.10.4. Wireless access point with antenna for the 61GHz unlicensed band. (Ubiquiti airFiber 60 LR. © Ubiquiti). The maximum transmission distance is 12Km.

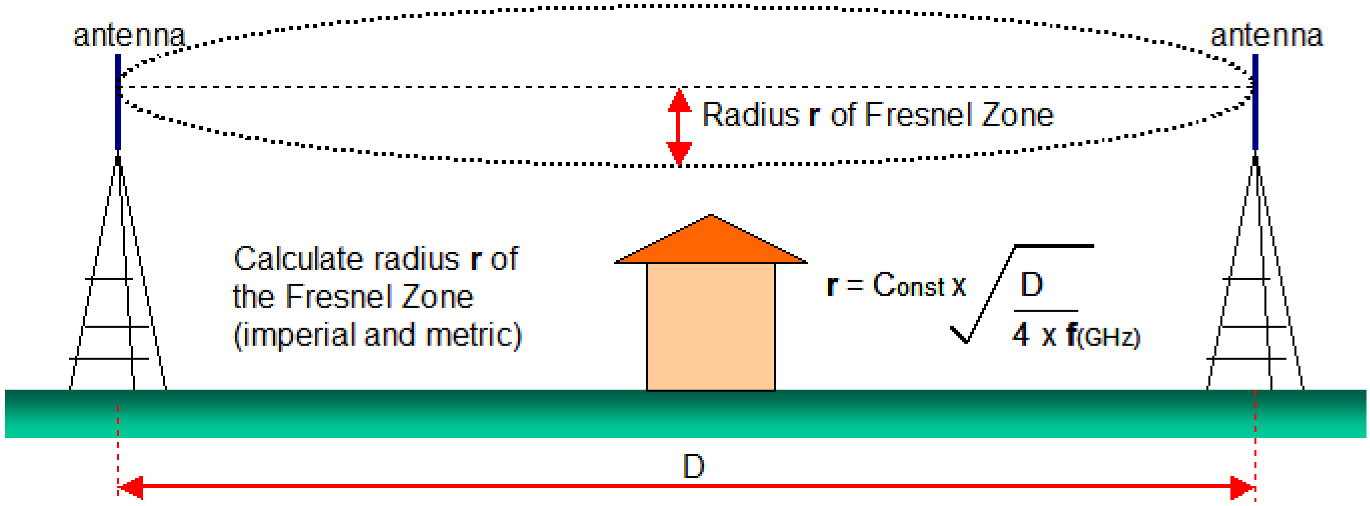
Parabolic antennas are directional with a narrow beam width and so alignment of the antennas takes time. One antenna will be the AP or head end, usually at the NOC, and the second antenna the client. In the WISP's network the NOC will be the AP and the tower will be the client, usually at the tower. Two technicians who are in radio contact make the alignment. First adjust the direction of the AP pointing it using line-of-sight. With the AP transmitting the SSID adjust the client antenna direction to maximize the signal strength shown on a computer connected to the antenna. The technician will be at the top of a tower doing this. Then the technician at the client end requests the technician at the head end via radio to make small adjustments to the direction attempting to increase the signal strength showing at the client.

2.11. Requirements for wireless links, the Freznel Zone

When constructing point-to-point (PtP) or point to multi-point (PtMP) line-of-sight wireless links there is an important factor to take into consideration that is essential for good communications; which is the Freznel Zone. There must be a clear space around the line-of-sight connection to ensure a good quality connection and be able to operate at the maximum distance. The space that must be maintained around the line-of-sight is called the Freznel Zone radius. Any obstacle in the path of the radio transmission within the Freznel will partially reduce the radio frequency signal strength by causing reflections and phase changes.

Is desirable to locate the PtMP antenna as high above the ground as possible to ensure that the Freznel Zone is clear. The formulas to calculate the minimum Freznel Zone radius are shown in the figure below. The distance **r** is the minimum distance between the direct line between the two antennas and the tallest obstacle in the path between the antennas.

For line of sight communications the FRESNEL ZONE must be clear of obstacles



Example (miles): distance D = 5 miles, frequency of link = 2.4 GHz

$\mathbf{r} = 72.05 \times \sqrt{5 / (4 \times 2.4)}$ = 52 feet, additional height of tower above obstacles

Example (Km): distance D = 5 Km, frequency of link = 2.4 GHz

$\mathbf{r} = 17.32 \times \sqrt{5 / (4 \times 2.4)}$ = 12.5 meters, additional height of tower above obstacles

Figure 2.11.1: Freznel zone calculation in imperial and metric quantities.

The formula for metric measurements requires the distance in Km, the frequency in GHz, which will give the maximum radius of the Freznel Zone in meters. The formula for imperial measurements requires the distance in miles, the frequency in GHz and will give the maximum radius of the Freznel Zone in feet.

If there are objects within the Freznel Zone then the antennas can be raised higher. For point-to-point backhaul links with Freznel Zone interference an intermediate radio relay antenna can be constructed to convert the path into two hops instead of one to provide clearance over obstacles.

When looking at the PtMP antenna from the CPE antenna site the visibility around the antenna should look approximately like the figure shown below.

Figure 2.11.2. Clear space around the antenna for the Freznel Zone.

2.12. Network interconnection components

There are several different types of network interconnection components that the WISP will require to build out the network. Some of these components are listed below.

- Routers.
- Switches.
- Power over Ethernet (PoE) supplies.
- Remote access power conditioners.

The router is a very flexible product and the WISP will need this for several points in the network implementation. Routers provide several network functions that may be required, these are listed below.

- Network address translation (NAT) between the LAN and WAN circuits.
- Dynamic Host Configuration Protocol (DHCP) service.
- Firewall rules, implement user rate plans, maximum speeds, data caps.
- Traffic monitoring and capture.
- Network component failure monitoring.
- Network monitoring using a SNMP (Simple Network Management Protocol) agent.
- API for remote access.
- UI for configuration.
- Command line console for configuration.
- Authentication of clients for access control, there are several methods including the use of an external RADIUS database.
- Dual WAN load balance and fail-over configuration for reliability.

A well-known router brand is manufactured by Cisco, with products that are known to be very reliable. However most WISP's find that Cisco products are too expensive for their budgets and choose lower-cost router products manufactured by Mikrotik. While Mikrotik products may not meet the Cisco quality standards, they do get the job done for an economical cost.

Routers have to be configured for the purpose they are required to serve in the network. Many routers have a graphical user interface for basic configuration, and it is necessary to load command line scripts to facilitate advanced router programming. Most routers also have a remote console or Application Program Interface (API) and some WISP cloud management products are able to communicate with routers directly to configure them so that the WISP does not have to learn the skills to configure routers.

Learning how to configure or program routers takes time. Cisco provides excellent training through the Cisco CCNA and CCNP Certification courses that require a student to dedicate 45 weeks. Mikrotik also provides excellent training for their RouterOS software through their Mikrotik Certified Network Associate Course (MTCNA) program.

A minimum of several months of work and considerable expense is required of someone who is already familiar with networking technology in order to complete these training courses. People who don't have a networking technology background should study networking technology before attempting a Cisco or Mikrotik Course.

Anyone who is Cisco Certified or Certified through the Mikrotik program will have no problem when designing, building and configuring a WISP network. An entrepreneur who wishes to start a WISP business, but who does not have the router configuration skills has one of two options;

- Employ staff that do have router configurations skills and trust that they are competent.

- Install management software or use cloud software that communicates with the router API interface in order to program the router directly.

Two types of routers are illustrated in the figures below. A later section of this book about the WISP network design will describe the router configuration requirements for WISP applications, including subscriber access control.

Figure 2.12.1. A Mikrotik router requires configuration via command line or UI, and also has an API for direct programming by WISP management software.

Figure 2.12.2. An easyWISP router designed for WISP's has no UI or command line, and is configured and managed by the cloud management software.

Network Ethernet switches are required to interconnect network components. One example shown in the next figure is a PtMP tower with two wireless access points that is connected to a client backhaul wireless via a switch. Ethernet switches will be installed at many points in the WISP network.

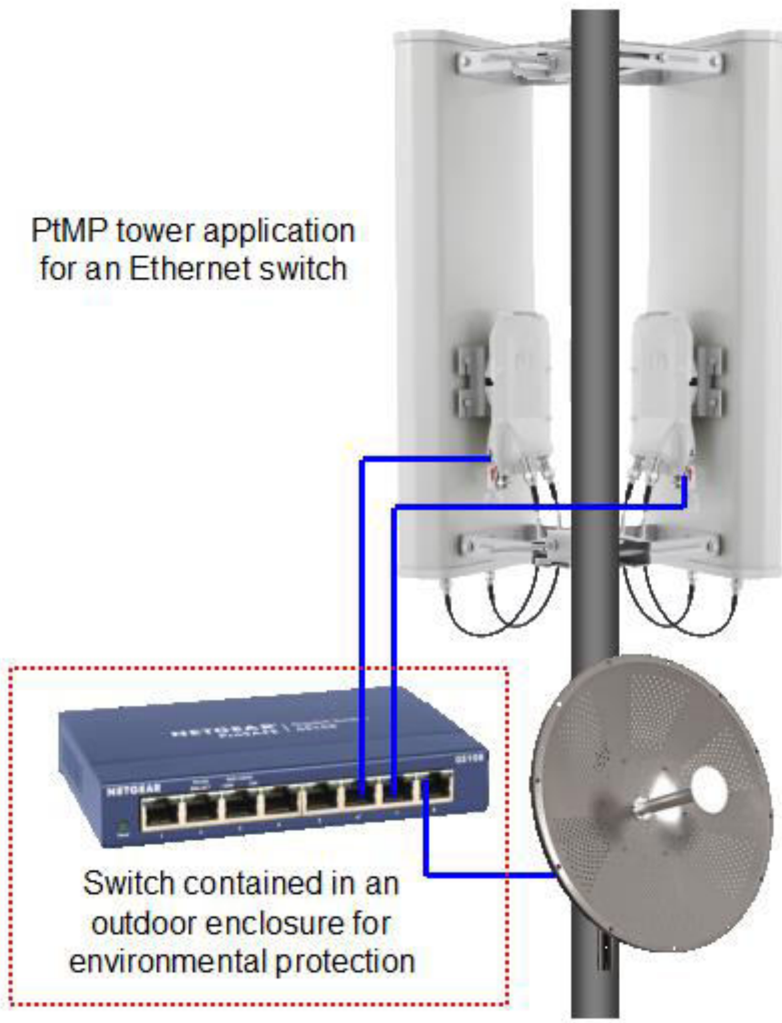


Figure 2.12.3. Application of an Ethernet switch installed at a PtMP tower.

The WISP should install switches that include support for the SNMP protocol permitting the device to be monitored from a central location. Monitored switches cost more but are very important to help ensure the reliability of the network and minimize downtime.

The WISP wireless equipment that is installed on towers or in premises is powered through the Ethernet cable as Cat6 cable has unused wire pairs, in addition to the wire pairs required for data. The Power-over-Ethernet (PoE) permits one cable to be run to the wireless device with both power and data. There are two common types of PoE, and each has several subtypes.

- IEEE 802.3af/at.
- Passive PoE.

Many manufacturers of telecommunications products for WISP's have adopted the IEEE 802.3af/at standard to power devices over the Ethernet data cable which connects the device to a switch or router. IEEE 802.3af/at is actually two standards.

- IEEE 802.3af, 48volt output up to 12.4 Watts, 258mA current.
- IEEE 802.3at, called PoE+, 48volt output up to 25.5 Watts, 531mA current.

PoE power supplies that are compliant with the IEEE 802.3af/at standard will not provide an output voltage until the signature resistance is detected in the Powered Device (PD) that is to receive the power. When the signature is detected the power supply enables 48volts to the device.

The passive PoE specification is not an International standard like IEEE 802.3; rather it is an informal standard that many manufacturers have agreed to adopt which powers equipment at 24 volts rather than 48 volts. The effect of this change is to reduce the manufacturing cost of products because power supplies that require a lower voltage can use components that cost less. Passive PoE does not have the safeguards that IEEE 802.3af/at has with regard to the load detection signature to enable the output voltage and does not sense the Powered Device to set the voltage, and supplies power at all times.

There are two types of PoE power supply, the mid-span device and the end-span device.

The mid-span device is a power injector that is inserted into the Ethernet cable. One Ethernet port, the LAN port, is connected to the network and is a conventional data port. The second port is a PoE Ethernet port that connects to the Powered Device (PD). The power is connected to two pairs of the cat6 Ethernet cable. Mid-span supplies are available for both 48volts (IEEE 802.3af/at) and 24volts Passive PoE. A mid-span device is shown in the figure below.

Figure 2.12.4. PoE mid-span power supply.

The end-span power supply is a PoE Ethernet switch which injects power into the Ethernet cable that is plugged into to the LAN port and connects to the Powered Device (PD), either 48volts (IEEE 802.3af/at) or 24 volts (Passive PoE). An end-span PoE switch is illustrated in the figure below.

Figure 2.12.5. End-span PoE switch.

The WISP should install a managed switch that has an SNMP agent as part of the network performance and failure monitoring functionality.

The application of mid-span power supplies is show in the figure, to connect a PtMP wireless access point to the client backhaul wireless unit.

The WISP should take care not to mix the two types of PoE equipment otherwise equipment damage may result.

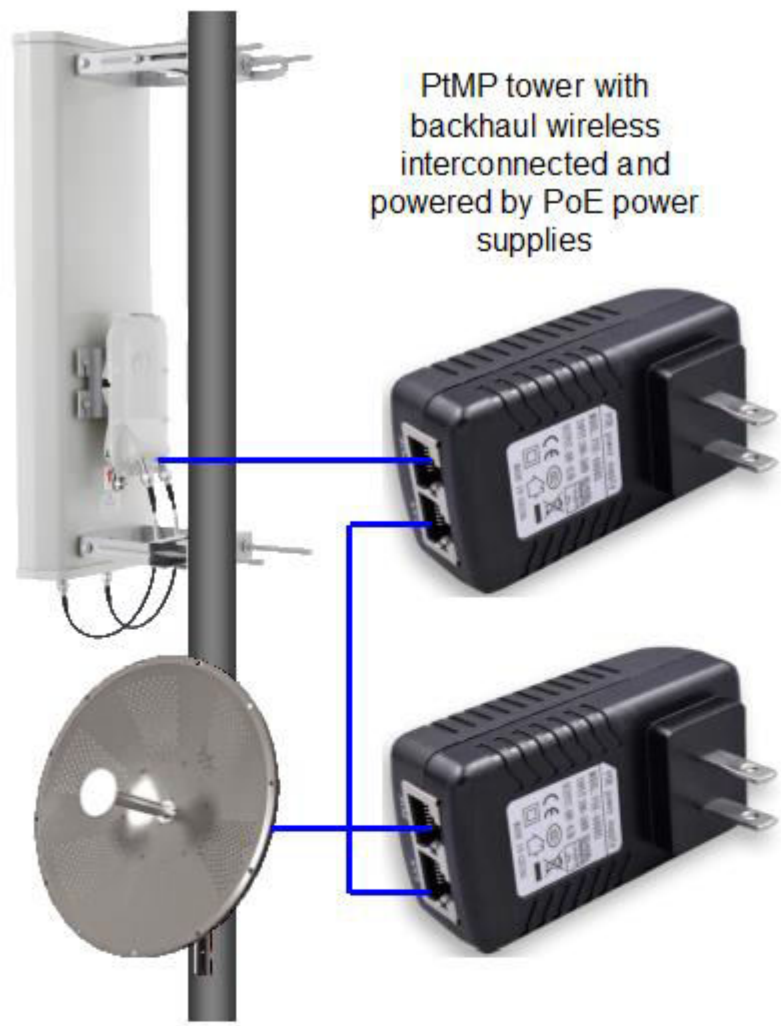


Figure 2.12.6. Connection of equipment with PoE power supplies.

Remote access power conditioners are essential for any type of remote installation, such as a PtMP tower. The remote access power conditioner has several features.

- Back-up power supply battery connection so that the network equipment will continue to function in the event of a power outage. The power conditioner will charge the battery while the power is available from an external source then switch over to the battery supply for power when the external power source is disabled.
- Remote control of each power port via the network so that the power to each port can be independently switched off then on to power cycle equipment connected to the port. This may be necessary to reboot equipment.

It is essential that remote locations like the PtMP tower have power backup and device power cycling, as any power issue will take time to repair because it will be necessary to travel to the tower site.

The central Network Operations Center location will also require a backup power source in case of a power outage. The WISP will be aware that the Network Operations center is a central point of failure. If a component fails or a power loss occurs in the Network Operations Center then all subscribers will loose their Internet service.

A remotely managed power conditioner is shown in the figure below. In addition to providing software that can remotely manage the electrical outlets, the product will have an SNMP agent so that its performance can be monitored by SNMP server software.

Figure 2.12.7. An example of a power conditioner with remote control to switch each power port.

2.13. Powering PtMP antenna locations

The point to multi-point (PtMP) wireless access points and point-to-point (PtP) wireless backhauls have to be installed at a high location, which can be the roof of a tall building, a tower or a hillside. In some of these cases electrical power is not available at the tower location. This is a common problem for Internet service providers. There are power kits available from many manufacturers, which provide the electrical energy for the installation. The power generation kit has four components.

- Solar panel, typically 100 watts.
- Wind turbine, typically 100 watts.
- Battery, typically 24 volts.
- Battery charger and voltage regulator that produces all voltages required by the equipment, and might be 12v, 24v, 48v and 110v.

The installation for the power generation equipment is shown in the figure below.

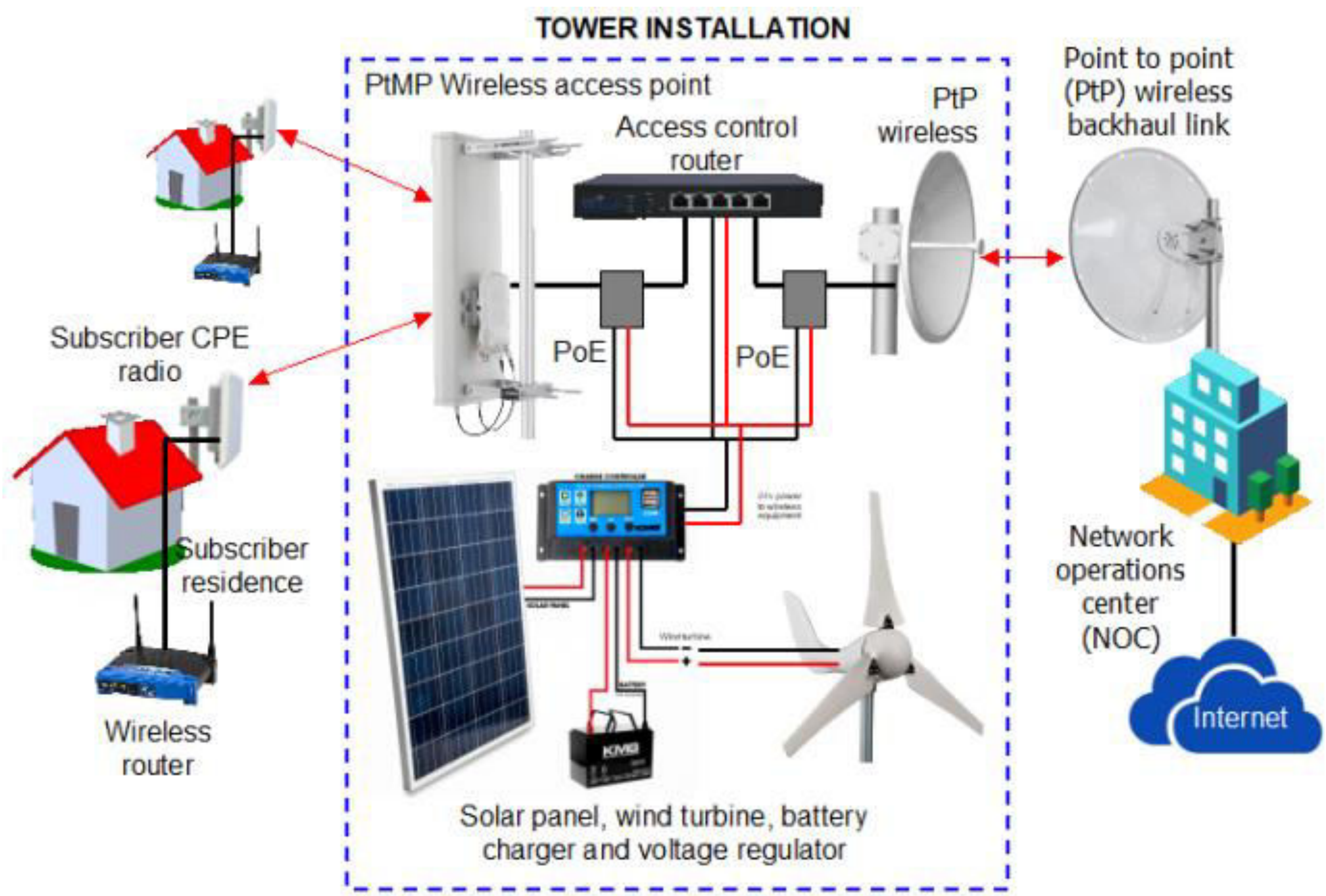


Figure 2.13.1. Power generation at the antenna site.

The battery charging and voltage regulating equipment has a connection for the battery, a connection for a solar panel and a connection for a wind turbine. Power is generated by both sources and the battery is charged at the charging rate specified for the battery. There are also regulated voltage outputs for the equipment that are provided by inverters, which take power from the battery. The equipment usually operates at one of four voltages.

- 12 volts, router and switch equipment.
- 24 volts, passive PoE equipment.
- 48 volts, IEEE 802.3af/at equipment.
- 110volts, router and switch equipment.

The status of power generation and battery storage can be monitored remotely over the network.

The wireless and access control equipment has low power consumption and will consume between 10 and 20 watts. The power generation and storage system can be designed for 100 watts of charging and use to ensure that the battery is always being charged. The Ampere/hour rate of the battery determines how long the equipment can operate without being charged. A battery can be chosen to power the equipment for one week so even when no power is being generated (night-time with no wind) there is a sufficient reserve of power stored in the battery.

If the wireless installation is a tower then an equipment housing is required at the base of the tower for the equipment and batteries. The PtMP antennas and backhaul antenna will be installed at the top of the tower for maximum line-of-sight visibility. The equipment housing will also require environmental conditioning. This may be a heater for equipment installed in a freezing climate, or a cooling fan for equipment installed in a hot climate. Some installations will require both due to a wide temperature swing between summer and winter. Finally some types of batteries will require venting. If low cost lead-acid batteries are used then an extractor fan is required to remove gasses produced by the battery.

The WISP should use the terrain where possible to locate the PtMP antenna. If there is a hill near the location where wireless coverage is desired then the PtMP antenna can be located on top of the hill. A hilltop location will eliminate the need to construct a tower.

The next figure shows a hillside antenna installation with solar panels and wind turbine that charge a large capacity battery. A point-to-point wireless backhaul parabolic antenna points towards the NOC location to provide the Internet connection. A point-to-multipoint sector antenna on the mast provides Internet access for the town's residents. A second parabolic antenna provides a forward link to a second PtMP site. The wireless Internet service provider has also installed an IP camera so that the site can be observed remotely. The equipment is tied down to a foundation in the ground to prevent wind damage. With any hillside installation it is always a good idea to install a fence around the equipment to prevent animals from damaging the equipment.

Figure 2.13.2. Hilltop PtMP antenna installation with backhaul antennas and solar panel plus wind power supply.

2.14. Outdoor and remote equipment protection

The PtMP and backhaul antennas are installed at the top of a tower or tall building for the maximum line-of-sight visibility. The drawback of having antennas installed at a high point is susceptibility of the installation to lightening strikes. It is not a question of if but when a lightening strike will occur.

All municipalities, states and countries have construction laws that determine how a lightening conductor should be installed on a tall building or tower. Any type of antenna installation will have to follow building rules and will require permits for construction. In the USA this means that licensed civil and electrical engineers will submit plans for the tower installation to the municipality for approval. The plans will include lightening conductors and grounding that follow the construction rules. During and after construction the municipality will send an inspector to approve the installation.

A lightening conductor is installed for the safety of people, and to prevent damage to structure in the event of a lightening strike. Not following lightening conductor rules is not an option; always install a lightening conductor. The WISP should be aware that a direct lightening strike will destroy all electronic equipment that the WISP has installed. In some parts of the world the permitting and approval process does not exist however the WISP is advised to implement lightening conductors for personal safety. Without lightening conductors the best outcome after a lightening strike is that all the equipment is destroyed, the worst outcome is that a person is at the site when lightening strikes.

The lightening conductor consists of three components, and the dimensions will be specified in the building regulations.

- A lightening rod is mounted at the top of the tower so that it is the highest point on the tower, above the antennas.
- A thick copper or aluminum cable runs the length of the tower from the lightening rod to the ground earth connector.
- An earth conductor is installed underground.

Figure 2.14.1. Antenna tower lightening conductor.

A lightening strike nearby to the location of the PtMP antenna may destroy the equipment because the bolt of lightening creates a magnetic field around it, and any metal wire that is within the magnetic field will have an induced EMF that can be upwards of thousands of volts. The WISP should install lightening arresters on any copper cable that connects to the equipment on the tower. Although fiber data cable is more expensive it will protect the equipment in the event of a nearby lightening strike. Power has to be provided to the PtMP antenna over copper wires and lightening arresters installed on the top and bottom of this cable are essential. Lightening arresters are not expensive and installing them does not add significant extra work. The safety of people and structures is very important.

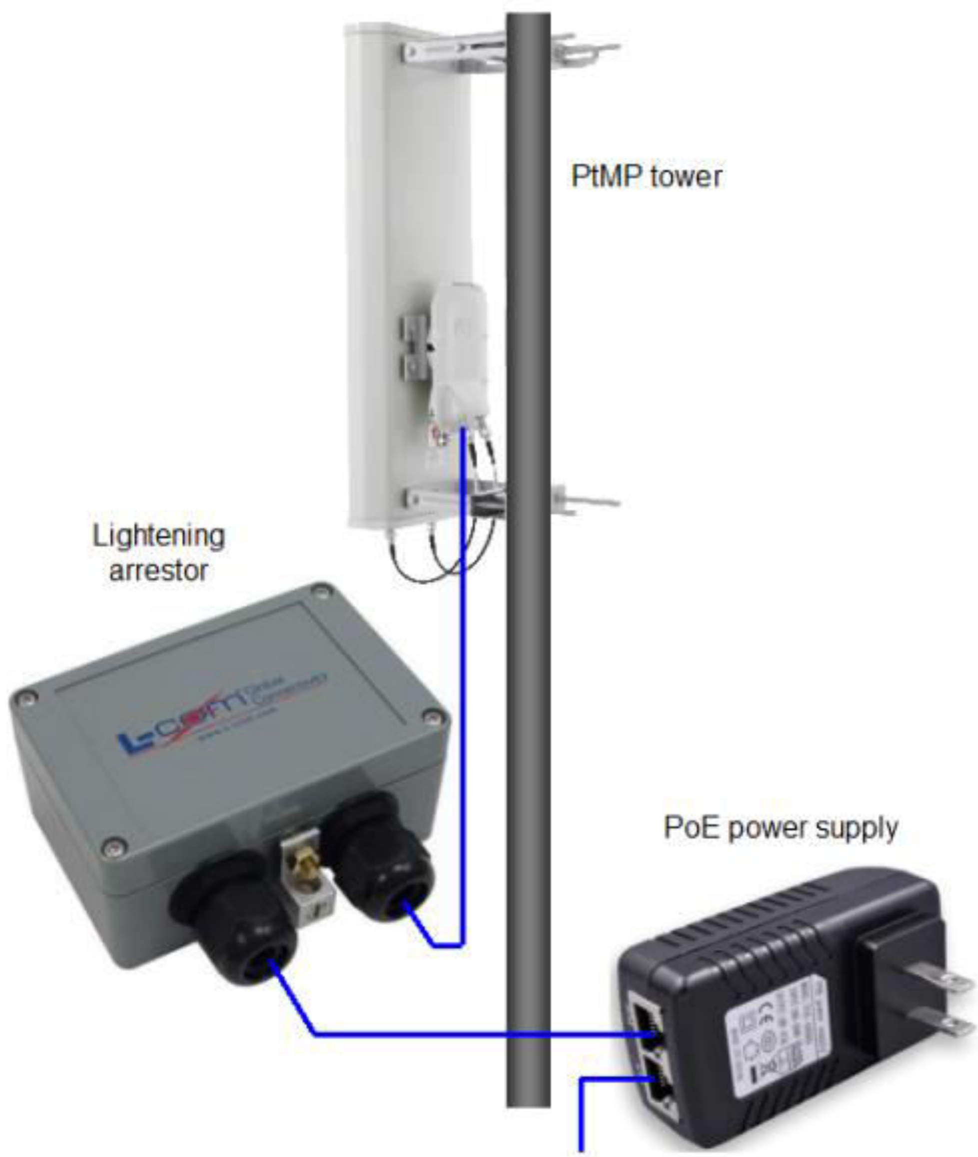


Figure 2.14.2. Ethernet data cable Lightening suppressor.

It is desirable to make environmental measurements at remote sites such as antenna towers and report these via monitoring software. Two important measurements are temperature and humidity. This is important where the equipment is used in winter conditions where the equipment room is heated to ensure that the equipment temperature does not drop below the minimum specification. Similarly when equipment is installed in a very hot environment it is necessary to cool the equipment. Temperature monitoring will provide an alarm if the temperature goes outside the desired range. Other quantities include power voltage and current, humidity and moisture, smoke and fire detection, and motion detection to alert the presence of a non-authorized person. Several manufacturers make remote monitoring equipment; one is shown in the figure below.

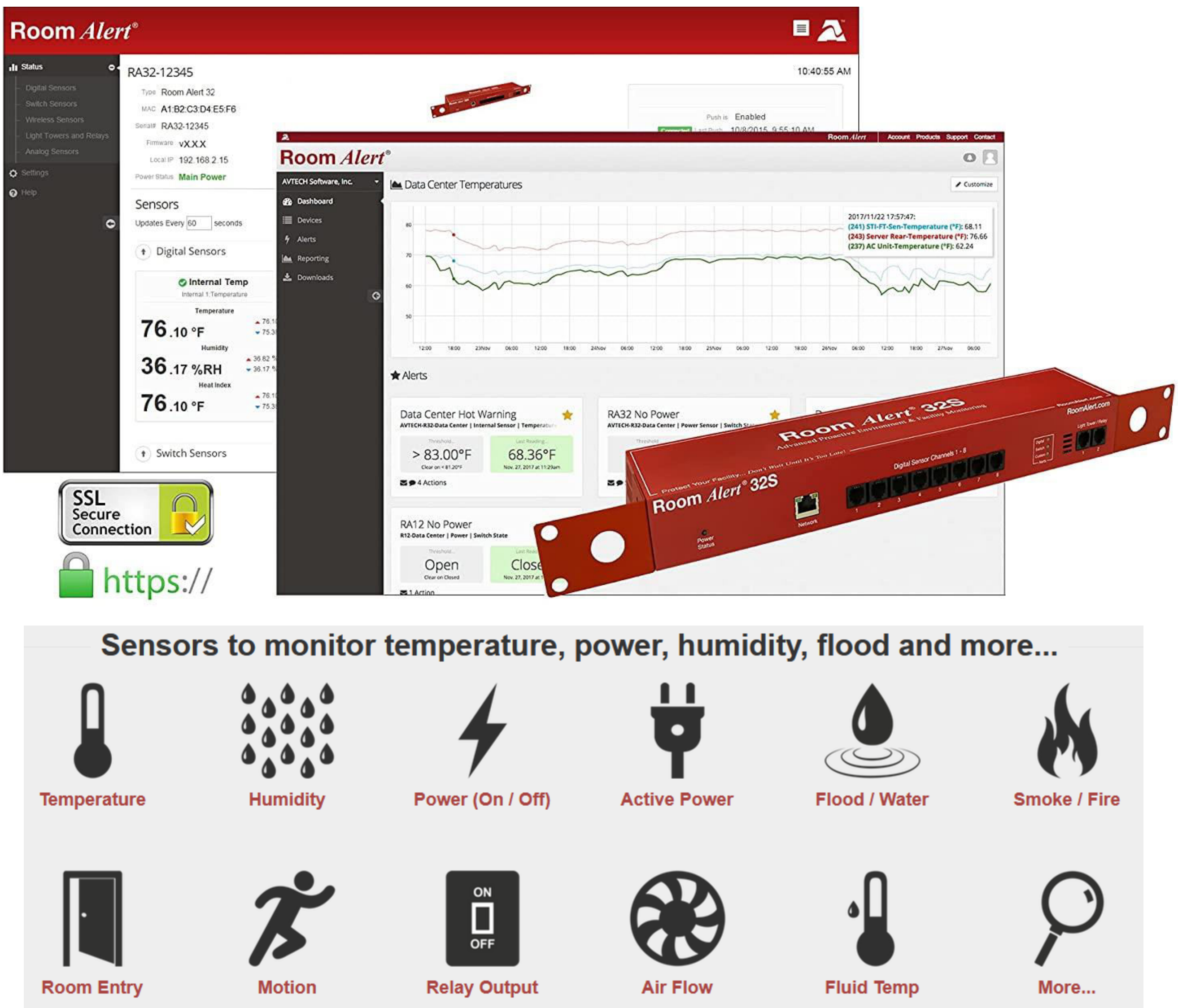


Figure 2.14.3. Environmental monitoring product.

In some locations, principally when the antenna tower is constructed close to an airport, it may be necessary to install a light on top of the tower as a warning to aviation. If this is the case then the municipal authority will provide the requirements for construction when the request for a building permit is made.

Figure 2.14.4. Antenna tower warning light for aviation.

2.15. Antenna towers

Antenna towers are part of a WISP's business but can be dangerous if the proper construction methods are not used. In the USA a building permit is required to erect an antenna tower. A civil engineer must calculate the foundation of steel and concrete that is required to support a specific mast height and weight. The foundation must be constructed first, inspected and approved by the building inspector before the antenna can be installed. The installation of the antenna must follow the instructions of the tower manufacturer to ensure that there is no weakness in the structure. The antenna construction must be inspected before the antennas can be installed. The inspector will verify the correct installation of a lightening conductor and any other local requirements such as a tower light. Some antennas will require guy-wires and then each guy-wire will require a foundation. A guy-wire is a tensioned cable that helps to support a freestanding structure such as an antenna tower.

In the USA an antenna has to be installed on a tower by a certified, licensed and insured tower climber. Certification training is required to obtain a license. The tower climber must also have the safety equipment such as a safety harness. It is likely that a permit will also be required to install an antenna on a mast. Although there is a lot of bureaucracy around the construction and use of towers the caution is necessary to prevent risks to workers and to the public.

Figure 2.15.1. A Rohm antenna mast, which is popular with WISPs.

Mobile antenna towers are also popular with WISP's for the reason that they can be erected quickly with less bureaucracy. A mobile antenna tower has a lower maximum height than a freestanding tower and so is suitable for installations where the additional height is not required.

The figure shows a mobile antenna in the process of installation and assembly. The tower lays flat on the trailer for transportation and is moved to a vertical position when installed at the desired site. As the antenna has no foundation four-trailer arms are swung out to stand on the ground and stabilize the structure through leverage. The mast consists of telescopic sections. After the antenna is installed the telescopic sections are moved up to their final height. Simple antenna trailers use manpower to move all the parts. Advanced trailers will have motors and hydraulic pumps to move the antenna tower components into position.

Figure 2.15.2. A mobile antenna mast mounted on a trailer.

2.16. Plotting the area of PtMP tower coverage

Before the WISP can start in business it is necessary to have a map showing the area where prospective customers have line-of-sight visibility from the customers premises to the PtMP wireless antenna. This is important because people will call to ask for the Internet service so the WISP must be able to respond that the customer can get a connection or not. If this is not done then the field service technician will have to visit every prospective customer who calls asking for service to discover if service can be provided.

The coverage map is prepared as soon as the tower PtMP wireless is operational. When the WISP is preparing the map it is necessary to identify the maximum range of the transmission around the antenna. The WISP can do the following.

- Evaluate the terrain to identify areas where there is no LoS to the antenna.
- Where there is LoS at a long distance use a CPE device connected to a laptop to measure the signal strength.

The resulting coverage map may look something like the figure below for multiple PtMP antenna towers.

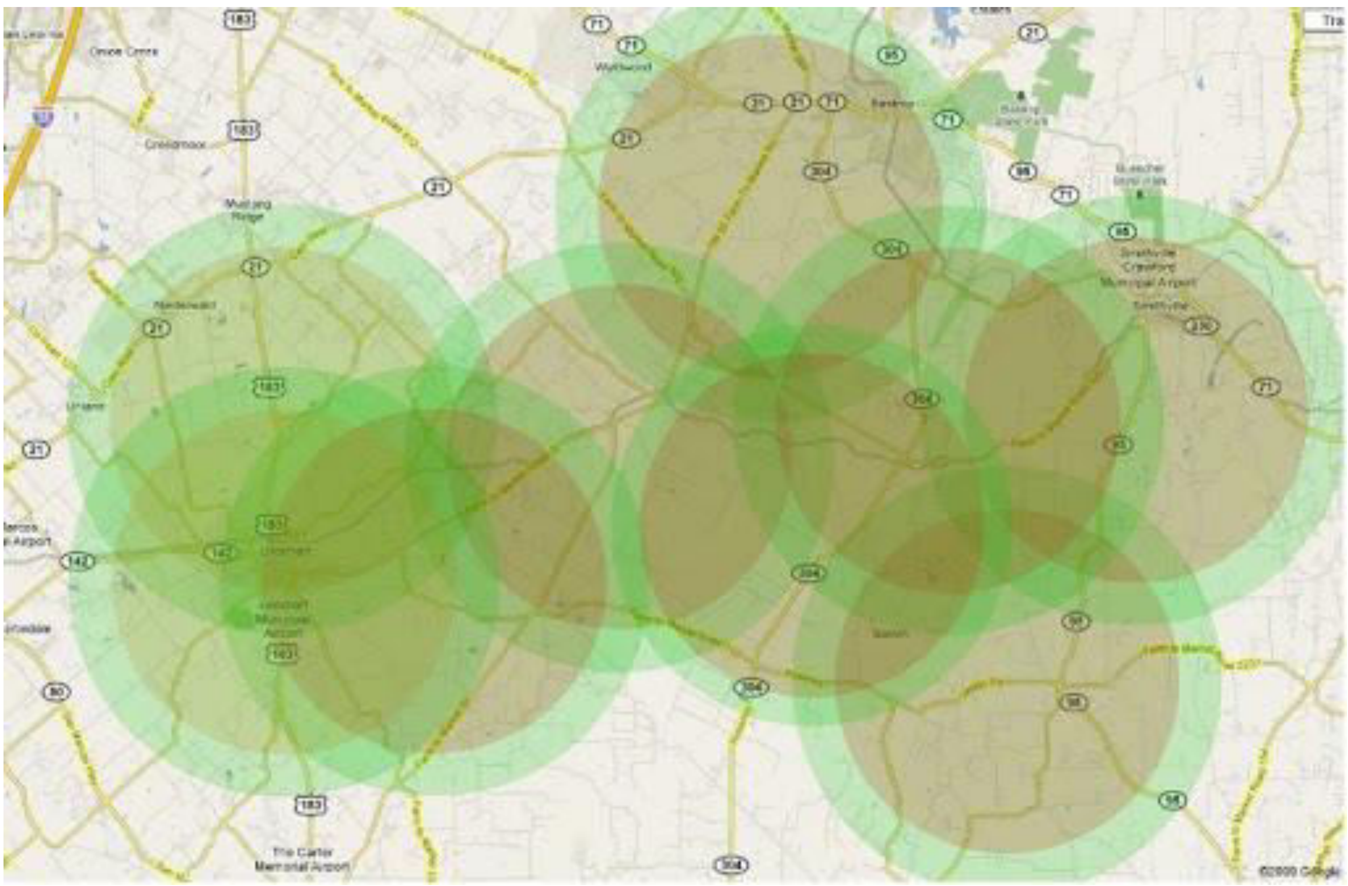


Figure 2.16.1. Map showing the RF coverage of each tower.

There are subscription services available in the USA that can plot the expected area of coverage onto a contour map. The WISP provides the tower location coordinates, tower height and transmission power in EIRP, this is the output power of the transmitter plus the gain of the antenna in decibels (dB). With the WISP's information the software will plot the approximate area of coverage for a CPE antenna to communicate with the

PtMP tower. This software cannot take into account the effects of season vegetation and so the WISP must inspect the area to evaluate the coverage area. The software subscription is quite expensive and only available for the USA. WISP's in other parts of the world will have to visit the terrain and evaluate the area of coverage.

2.17. Contention ratio

An operational parameter that is very important for WISP's is the contention ratio. The contention ratio is the degree to which the sale of Internet bandwidth exceeds the bandwidth that is available and describes how an Internet service provider can oversell the backhaul capacity with minimal degradation of each customer’s Internet service. Overselling backhaul network capacity is beneficial for the WISP because it will increase the profit of the wireless Internet service provider business.

All Internet service providers oversell capacity because the probability of all customers connecting at the same time with each one using the maximum data capacity is very low. However if that should happen then the Internet data speed for each subscriber will be degraded.

Internet Service Providers have contention ratios for each group of subscribers, but they don't publish the values. For example, residential customers might have a higher contention ratio than business customers who are charged more for the Internet service. A subscriber can verify that the connection speed at peak time of network use will fall below the maximum speed that the customer purchased. The fine print of the WISP’s agreement with the subscriber will advise that the contracted data speed may vary from the maximum speed.

The WISP must evaluate the quality of service provided to customers to determine the ideal contention ratio. The WISP has to find the right balance between profitability and avoiding a noticeable deterioration of the customers Internet service, which will cause complaints. The contention ratio is a factor that affects the profit and loss statement.

In practice, most subscribers will be downloading much less than their maximum data speed limit because they are checking emails or interacting on social media. For this reason an ISP can have a contention ratio of 5:1 and not be concerned that subscribers will complain about the slow service. However if the subscriber is streaming video from a service like Youtube or Netflix then it is possible to reach the maximum speed that the subscriber is permitted to download. Telephone Voice-over-IP (VoIP) services also consume considerable bandwidth, though less than video streaming. For this reason some ISP's set a different maximum download speed for video streaming and VoIP, which might be half of the maximum permitted download speed for other applications. This procedure is called data shaping and the differential data speeds are programmed into the access control router.

The following example explains the exact meaning of contention ratio. A wireless Internet service provider tower has a backhaul of 100 Mb/s. The Internet service provider sells rate plans of 5 Mb/s to subscribers. This means that when 20 subscribers are connected to the network and each is using their maximum data capacity of 5 Mb/s then the backhaul circuit will be operating at the maximum data capacity of 100 Mb/s. In practice not all subscribers will be connected at the same time, and many of the connected subscribers will not be using the maximum data capacity. Data capacity use depends on the type of application being used. Email will generate a very low aggregate data rate while video streaming will generate the maximum data rate. Voice and video over IP (VoIP) applications will generate a high data rate. Knowing the data use characteristics of subscribers it is possible to oversell the backhaul capacity by a contention ratio of 5:1 or greater. With a contention ratio chosen of 5:1 then the 100 Mb/s backhaul capacity can be sold as 500 Mb/s capacity. This means that 100 data rate plans of 5 Mb/s can be sold to subscribers.

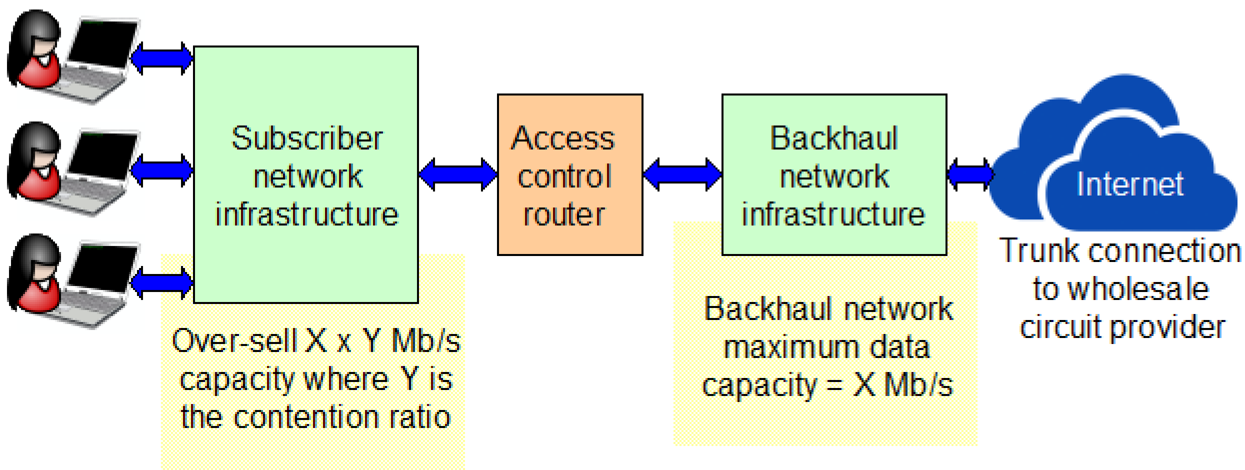


Figure 2.17.1. Overselling backhaul capacity and the contention ratio.

There are simple rules for maximizing the contention ratio in order to improve the business profitability.

The rate plan that is sold to subscribers should be a very small fraction of the backhaul capacity. For example, with a backhaul of 100 Mb/s then it is not possible to sell the service to more than one subscriber if the rate plan is 100Mb/s. The contention ratio can only be 1:1 as adding a second subscriber with the same rate plan will cause the data rate of each subscriber to fall to half when both are streaming at maximum data speeds.

However if the Internet service provider sells data rate plans of 5 Mb/s then there is a high probability that only a small proportion of the subscribers will be connected at one time, and not all connected subscribers will be using high data rates. The Internet service provider can then sell a 5 Mb/s service to many more subscribers than the theoretical 20, possibly to 100 5Mb/s subscribers with a contention ratio of 5:1. In practice the Internet service provider will offer several rate plans, from low cost low speed plans to high-speed high cost plans. The Internet service provider should try to concentrate sales to more customers at the low cost low speed end of the scale so that the contention ratio can be increased which will increase profits.

WISP’s estimate that a customer with a high network bandwidth will consume approximately 4Mb/s at peak times due to the applications that the customer uses, such as video streaming (Netflix) or VoIP (Skype). The WISP can therefore use this figure to calculate contention ratios.

2.18. Network performance and failure monitoring

The reliability of the WISP network is extremely important as any downtime will cause customers to call with complaints, and frequent downtime will cause customers to cancel the service or switch to a competitor, which is called churn in the telecom industry. Avoiding or minimizing downtime depends on three factors.

- Install reliable equipment that has support from the manufacturer. The quality of the network installation and components that are installed in the network will determine the reliability of the network.
- Install a back-up supply that has instantaneous switch over when a power failure occurs and will keep all equipment operational for several hours during a power outage. Loss of power can occur during bad weather.
- Install failure-monitoring software that monitors all equipment so a failure is detected immediately when it occurs and can be repaired quickly. Continuous monitoring of the network to identify problems that might cause downtime must generate an alarm when a component failure occurs and a fast repair is essential to minimize network downtime.

There are many different types of network monitoring software. Some are free to use and the WISP can install without charge, some are open source and can be modified by the WISP, some are for a specific brand of network products, and some charge a fee for the software but provide a service. A list of monitoring software providers is included in the references at the end of this book.

Most monitoring software for networks uses a monitoring method called the Simple Network Management Protocol (SNMP), which is part of the Internet Protocol Suite that was defined by the Internet Engineering Task Force (IETF).

SNMP has two components.

- The SNMP Agent; the agent is software that is installed in each network device, it maintains a record of network data in a table called the Message Information Base (MIB) and provides this information on request.
- The SNMP Manager; the software installed on a server computer at the network operations center or some other location that continuously polls (calls) each SNMP agent and collects the MIB Information from each agent. The collected information is displayed on the software screen. If a device does not respond to the SNMP request then an alert is given to the network administrator that a device has failed to respond. The SNMP manager software is configured with the IP address and port number of each device that will be monitored. It will usually be necessary to enable SNMP monitoring on each device to allow the SNMP agent to be accessed by the SNMP manager. The SNMP agent listens to requests coming from the SNMP manager on the UDP port 161, while the SNMP manager listens to alarms “TRAP” coming from the agent on port UDP 162.

Many types of network products include a Simple Network Management Protocol (SNMP) agent and the WISP should ensure that any equipment that is purchased is capable of being monitored using SNMP manager software. The SNMP manager will poll each device with an SNMP agent to check the device status then display that information on the computer screen. Some WISP management software includes a network monitoring and failure-alerting feature. Some cloud vendors include failure monitoring and alerting as part of the service they provide. The monitoring can either be a proprietary system or based on SNMP. When the WISP is selecting business management software or a cloud service preference should be given to products that include network monitoring and failure alerting features.

Each SNMP client maintains a MIB table where operational parameters are saved and updated. The SNMP server communicates with each remote device in sequence and compiles all the information received into a series of displays like the one shown below. If a device fails to respond then an alert is issued to the administrator that a problem has occurred.

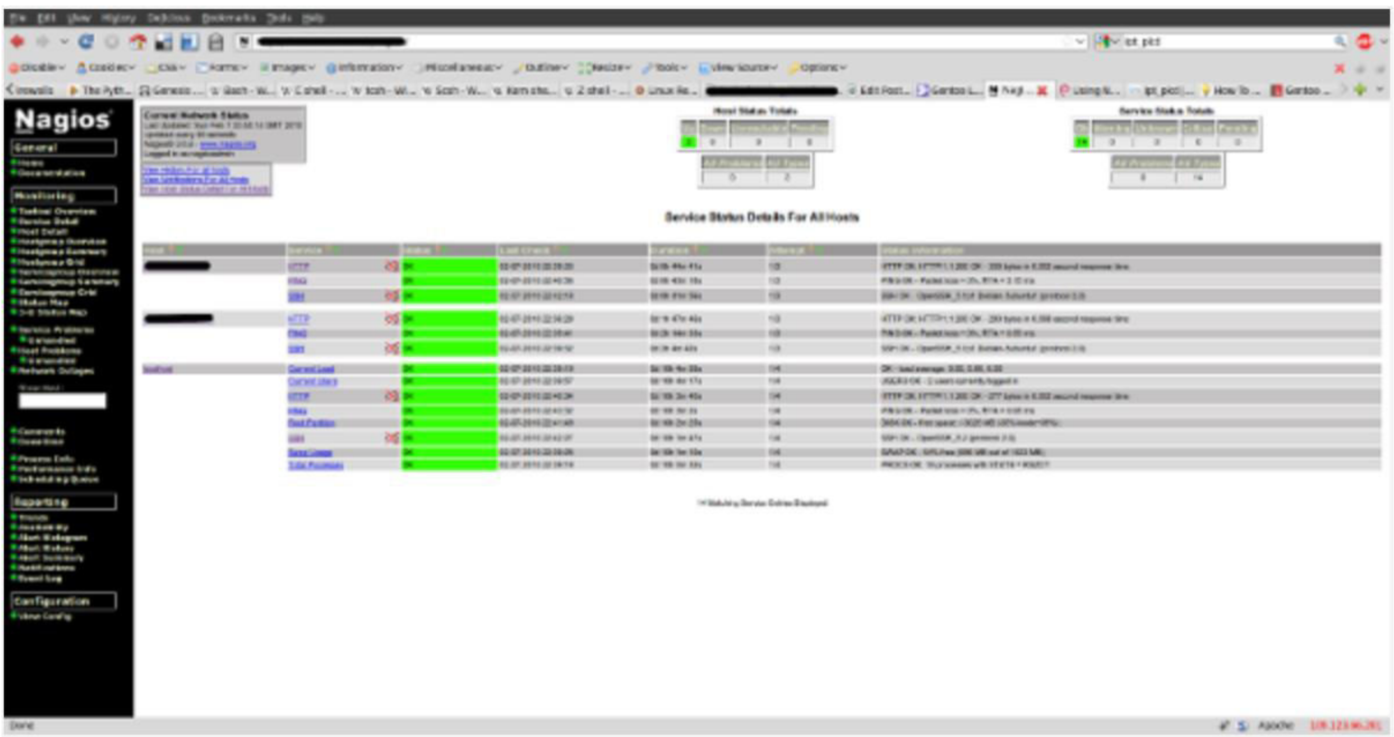


Figure 2.18.1. Open-source SNMP software monitoring display.

When designing and building the network the WISP should ensure that all monitored device IP's are accessible from the network operations center. If routers are part of the network design then it will be necessary to configure port-forward rules on each router so that the SNMP manager can access SNMP device agents behind the router.

A desirable feature that the monitoring software should have is the ability to test the network circuit through to the CPE wireless installed at the customer's premises. This feature is important for customer support staff. Often a customer will call the WISP customer support line and advise that they have no Internet. The customer support staff should be able to test the circuit through to the CPE to advise the customer if the problem lies in the WISP network or there is a problem with the customers network installation. The result of the test will determine the course of action. If a problem is found in the WISP's network then the support staff will issue a maintenance request to the field service technician. If the problem is found in the customers network the WISP should have a policy in place to charge the customer for a technical visit to repair the installation.

The diagram below shows the network installation with the SNMP manager monitoring software communicating with every device that has a SNMP agent installed.

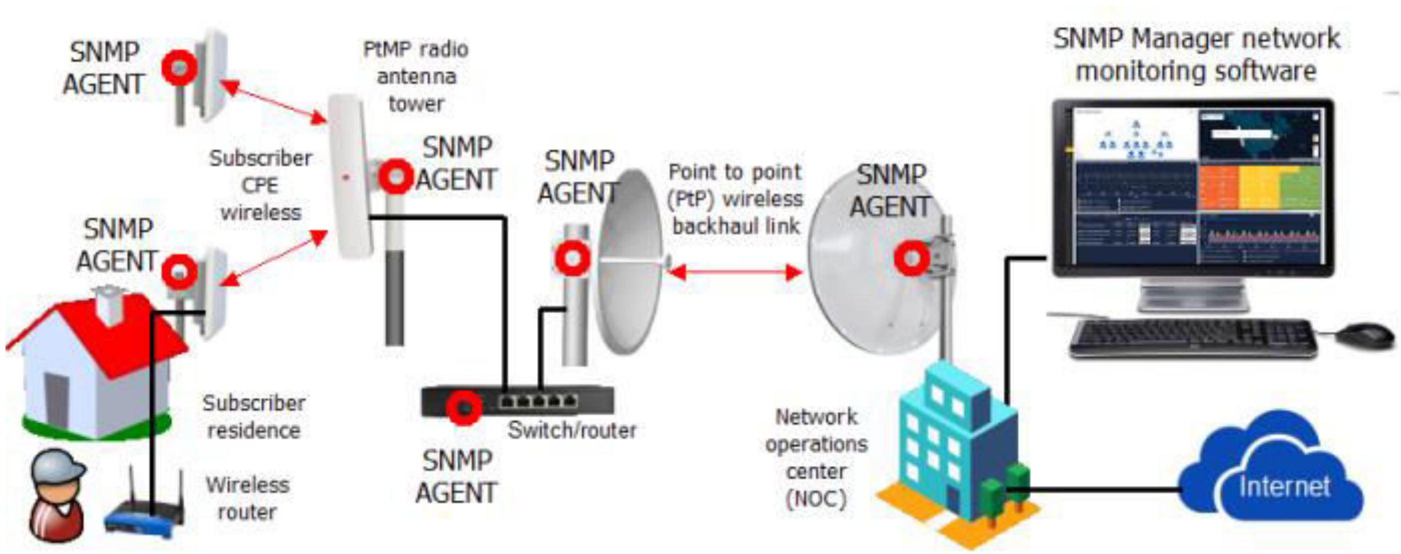


Figure 2.18.2. Network monitoring software uses the SNMP protocol. Each red circle represents the SNMP agent software within a device.

It is impossible to prevent failures from happening as the causes may be outside the control of the service provider but it is important that any failure is corrected quickly with minimum downtime for the customer. The WISP must develop a procedure to quickly repair defective products. This may include having a technician on standby 24/7. When the monitoring software issues an alert that a component has failed then a work order must be issued immediately to the field service technician to proceed with the repair.

2.19. Network congestion

One of the tasks of the network monitoring software is to compile information for each data link. A data link might be a point-to-point wireless link that connects the PtMP tower to the NOC. The information that is gathered is the data throughput of each data circuit as a percentage of maximum possible data transmission plotted with time. Data transmission information is collected for each data link as shown in the diagram below.

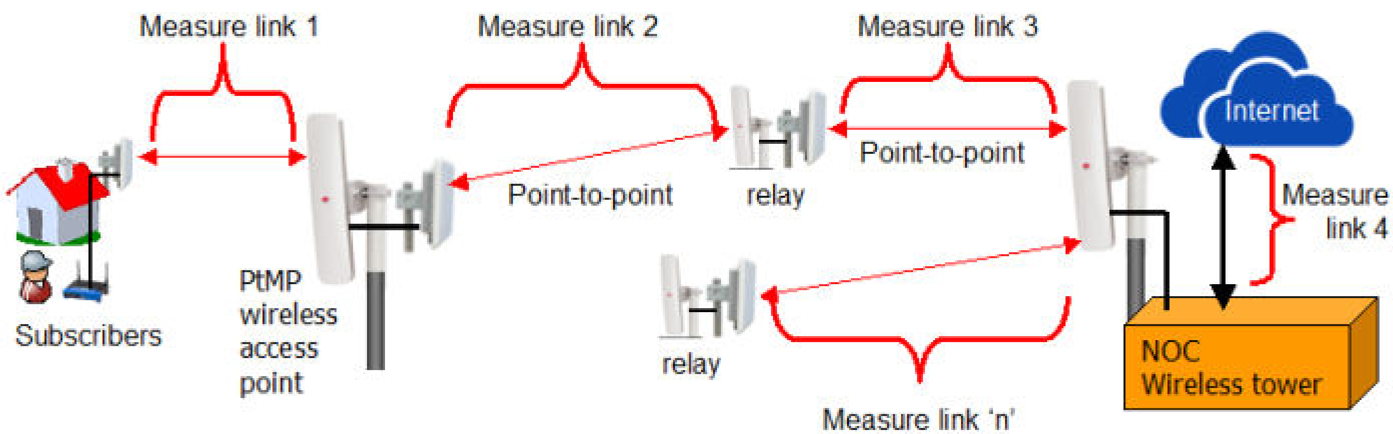


Figure 2.19.1. Measure the performance of each data link in the network.

It is important to view how much of each link available bandwidth is being used. If the use is constantly at 100% during peak hours then it is possible that network congestion is occurring at that time. Network congestion occurs when a network link is carrying the maximum amount of data that the circuit bandwidth permits and the demand on that circuit is greater than the maximum bandwidth. When this occurs data packets are queued waiting for transmission and so there is a transmission delay and possible data packet loss, which reduces the quality of service. Network protocols retransmit data packets when packet loss occurs which increases congestion to the point where circuit failure occurs and data transmission stops for a period of time until users are disconnected and the circuit recovers. This situation is called congestive collapse and will cause customers to loose the Internet connection.

An example of a time varying graph showing network link utilization is presented in the next two figures. The first graph shows a network connection that is operating at half maximum capacity and so there is no risk of network congestion. The next graph shows a network link that is operating at maximum capacity for much of the time and so the link will exhibit network congestion. When the WISP observes a graph such as this then the circuit capacity must be upgraded to avoid the risk of congestive collapse and the subsequent disconnection of customers from the Internet.

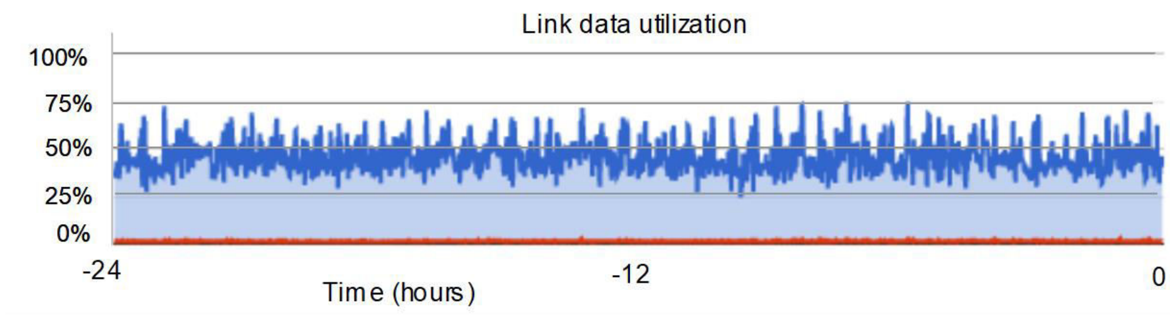


Figure 2.19.2. An example of network link utilization as a percentage of bandwidth available. The data link utilization is approximately 50% of maximum capacity.

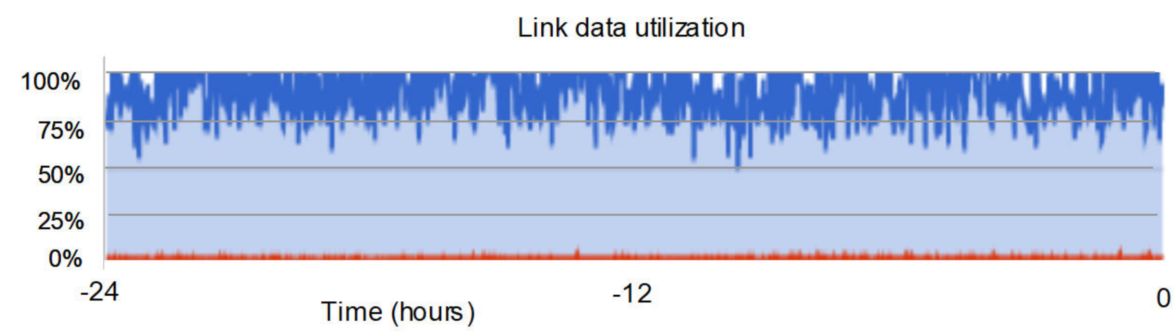


Figure 2.19.3. An example of network link utilization that is approaching network congestion. When congestive collapse occurs the data link traffic will drop to zero for a short time. The data link capacity must be increased with this situation.

2.20. Radio frequency interference

Many WISP wireless networks will be installed using unlicensed frequency equipment for low cost. Each communications link will be subject to interference from other devices that use the same frequencies. When the WISP installs the wireless equipment a scan should be made across the unlicensed frequency spectrum for other sources of radio frequency radiation that might interfere with the WISP's wireless link. The scan is made using a tool called a spectrum analyzer. The WISP should configure the wireless equipment to use the frequency with the least interference.

The WISP has to maintain continuous vigilance of all wireless links because as time passes other people will install equipment, which will interfere with the WISP's wireless link. Monitoring the equipment that is part of the wireless link using SNMP will provide information about the ongoing quality of the link. Keep a log of the signal to noise ratio of the wireless link and watch for deterioration, which may be an indication of interference from another source. In the worst case the link will stop working without explanation due to interference. When the WISP goes to the tower site to investigate any link connection problem a portable radio frequency spectrum analyzer should be included in the toolkit to scan for interference. It may be possible that changing the link frequency solves the interference problem. The likelihood of interference in the 5.8GHz band is less than the 2.4GHz band so the 5.8GHz band is preferred for wireless links wherever possible. Rural areas will have much less interference than urban areas. It might be impossible to avoid interference across the unlicensed bands in urban areas and so the only solution is to use licensed frequency bands.

When connecting residential and business buildings in a dense urban area there will always be interference from transmitters that are using the same unlicensed frequencies. One of the worst offending equipments is the cordless phone that transmits a high power signal right across the unlicensed band, not just at one frequency. Business security cameras that have an RF connection to the base station instead of a cable connection also cause serious interference. The camera RF transmitters radiate a strong signal across the whole band usually through an omni directional antenna. It is surprising that such equipment has FCC approval and that the equipment is sold without instructions for correct installations use to minimize interference for others. IP cameras that are designed for IEEE 802.11 networks and transmit on a specific channel do not cause interference.

A wireless access point and CPE receive a band of frequencies, not just one frequency, because the IEEE 802.11 transmission requires a band of frequencies in order to transport the data at high data rates. The transmission uses a modulated carrier where the transmission is centered on one frequency but the data modulation spreads the transmission over a band of frequencies. The receiver sees any and all transmissions within the band of frequencies that it is designed to receive. Unwanted transmissions are received as noise and so the receiver has to separate the wanted signal from the unwanted noise. The noise is the interference that causes the reduction of the signal-to-noise ratio in the wireless receiver because the background interference strength is measured in relative to the strength of the wanted signal. As the background noise increases, the signal-to-noise ratio reduces, which makes it harder for the receiver to separate the data transmission from the noise. When this occurs the IEEE 802.11 standard has design features to attempt transmission at a lower data rate. Both the transmitter and receiver switch to a lower data rate in order to maintain communications. As the noise interference increases the data rates switch to lower and lower speeds until the noise level is equal to the signal level and communications is no longer possible. Conversely a high signal to noise ratio means that the received signal is very strong in relation to the background RF noise and can support a high data rate.

There are some techniques that will help to reduce interference.

The 2.4GHz unlicensed band has a lot of interference however the 5GHz unlicensed band is much broader with more channels available and so it is possible to find unused RF (radio frequency) channels in that band. Use a spectrum analyzer to investigate and identify 5GHz band frequencies that have less interference. The WISP can also identify IEEE 802.11 transmissions using a mobile phone that has 5GHz WiFi with free software from the app store such as WiFi Analyzer. This method will detect the transmissions from IEEE 802.11 devices but will not detect transmissions from other devices such as cordless phones, which are the worst offenders. RF spectrum analyzers that cover the 2.4GHz and 5GHz bands tend to be expensive, however low-cost portable products that use a popular tablet are available.

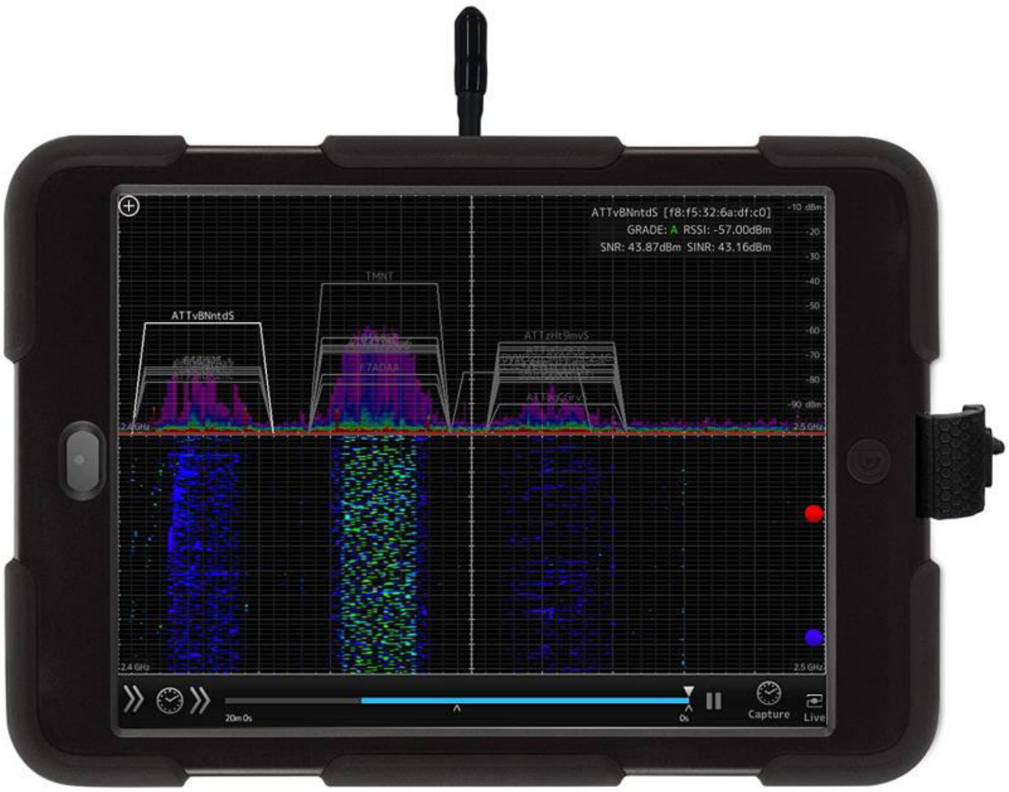


Figure 2.20.1. A low-cost portable spectrum analyzer for 2.4GHz and 5GHz.

The second solution is to use a very high gain directional parabolic antenna for point-to-point links that will reduce interference from sources that are transmitting around the antenna being used for communications. This is because the beam width is very narrow with a high gain antenna so the wireless only receives RF signals that are within the narrow beam path. The best antenna combination for PtMP is to use a high gain parabolic antenna with the CPE wireless and a sector or beam-forming antenna with the PtMP wireless.

Employing the two methods described above will solve most RF interference problems. However in the rare cases where interference prevents data transmission then the alternative is to pay to use a licensed frequency. Government agencies, such as the FCC in the USA, are responsible for the allocation of licensed frequencies and the sale of licenses. A license will usually require an annual payment to operate on the frequency allocated. The advantage of using a licensed frequency is that if the licensee has a problem with interference then a complaint can be filed with the licensing authority. It is unusual for a licensed frequency to be used without a license however FCC engineers can detect this occurrence. Any unlicensed transmission in a licensed frequency band will result in the offending equipment being confiscated. An additional cost of using a licensed frequency is that the wireless equipment is more expensive than equipment for unlicensed frequencies as the manufacturing volume is very small.

2.21. Summary

The key points or take-a-way's that an entrepreneur should remember when evaluating technology for a WISP business are listed below.

- For a low cost of investment and operations use wireless equipment for the unlicensed frequencies of 2.4GHz and 5.8GHZ, for both PtMP and PtP. Both frequencies are line-of-sight, and blocked by obstacles so a site survey is essential.
- 2.4GHz has lower cost and higher interference; 5.8GHz has slightly higher cost and lower interference.
- The 5.8GHz band permits higher data rates than the 2.4GHz band due to the availability of more frequency channels.
- When planning to provide a fixed broadband service determine first how the customer will be charged for the CPE installation, up front payment or amortized in monthly payments.
- Before offering a fixed broadband service prepare a subscriber agreement.
- When planning to begin a mobile broadband service select the payment methods to be offered, including cash payments.
- Ensure that a mobile broadband service supports mobility so that users can move between antennas at different sites.
- A mobile broadband wireless service is not encrypted so ensure that the access control router has protection from hacking.
- When evaluating wireless access point antenna types don't choose omni-directional. Sector antennas are best but sometimes expensive, Ubiquiti has low cost 5GHz WAP's with sector antennas (used by the author).
- Choose the PtMP antenna location carefully following the criteria for line-of-sight both for the customer CPE's and for the backhaul to the NOC.
- When there is no line-of-sight from the PtMP tower to the NOC plan the installation of relay/repeaters required for LOS to the PtMP tower.
- When installing client premise equipment (CPE) choose a patch antenna for short distances because it is low cost and quick to align. Choose a parabolic antenna for longer distances for the best communications quality and high data rates.
- Prepare a client premise installation kit for premises CPE and networks.

- Use parabolic antennas for point-to-point wireless links for the lowest interference, highest signal strength and highest data rate. Take care with antenna alignment.
- For higher bandwidth point-to-point links (Gbit/s range) install unlicensed spectrum 24GHz and 60GHz links.
- For PtMP and PtP links take care with the Freznel Zone calculation, ensure no obstacles are in the wireless transmission Freznel Zone path.
- Look for wireless products and network interconnection components, routers, switches, etc that have an SNMP agent and can be monitored for performance and failure. Network performance and failure monitoring is essential for reliable infrastructure. Use free or paid SNMP manager software.
- Plan for power generation equipment for the remote PtMP tower site, if the tower location does not have power.
- Equipment protection is essential; lightening, static discharge, and environmental monitoring. Make sure to follow local construction laws when installing PtMP and PtP antennas.
- Antenna towers are a big investment and need a substantial foundation, have a civil engineer check the plans and give advice.
- The contention ratio is key to profitability, calculate and optimize for maximum return on investment.
- Failure monitoring is essential for a service provider and should always be included in the network design and the budget.
- Throughput monitoring of each data link is essential to check for network congestion.
- Be prepared to manage wireless interference problems when installing a wireless network, especially in an urban area.

3. Fixed and mobile broadband access control

3.1. WISP Internet service provisioning and access control

The Wireless Internet Service Provider (WISP) installs wireless network infrastructure that will connect a customer to the Internet. The access control is an integral component of the network infrastructure. Access control is like a water tap that can turn the flow of Internet data to the customer on and off, and can regulate the flow of data from slow to fast. The access control can also disconnect the customer after a specified amount of data has flowed through it, or if the payment for the service is not made. Access control is essential to manage the delivery of the Internet service to the customer and when combined with WISP management automation is a key element to grow the WISP business and manage it efficiently.

The access control rules are implemented for each customer using an access control router. The access controller can be implemented using a general-purpose network router that has been configured using a router scripting language, or can be a dedicated access control gateway with custom designed access control software. For an equivalent hardware cost the dedicated access control gateway provides a higher performance than the general-purpose router. Configuring a general-purpose router requires technical knowledge of router programming. Some WISP management software can communicate with the router API (application program interface), to simplify the programming task. A custom designed access control router will be a peripheral of the WISP management software that controls the unit.

An Internet service provider has three methods of charging customers for the service; pre-pay subscription, post pay subscription or pre-pay-on-demand. Pre- and post-pay are fixed broadband subscriber options for the customer making regular monthly payments, however pay-on demand can be an anonymous mobile broadband customer who is purchasing Internet access as required.

- Pre-pay subscriber with fixed broadband; the customer pays for a calendar month of services on or before the start date of the billing period.
- Post-pay subscriber with fixed broadband; the customer pays for a calendar month of services after the completion of the billing period with a maximum limit to receive the payment, usually 30 days.
- Pre-pay-on-demand customer is most often an anonymous user of mobile broadband; the customer pre-pays for an amount of Internet access, which may be of a fixed duration or of a quantity of data, or both.

Two types of access control methods are required if the WISP offers both fixed broadband services for pre-post-pay customers and mobile broadband services for on-demand payment customers.

Access control technology has to implement several features that ensure that the data service provided for the customer is reliable and meets the agreement made with the customer. The tasks implemented by the access control router for fixed broadband pre-pay and post-pay subscribers are listed below.

- Authenticate a user by verifying that the user is legitimate. One of several authentication methods can be implemented to authorize the customer onto the network.
- Activate a new customer when added to the billing system and then deactivate a customer if necessary, according to the status of the account payment, if the account is not paid by the due date the customer is temporarily deactivated and disconnected from the Internet but can still access the CRM system. When the account is paid the customer is re-activated.
- Application of the rate plan that was chosen by the customer based on the cost of the plan vs. the desired data speed. Rate plans include the maximum download and upload data speeds, may include a rate cap and may include QoS (quality of service) to differentiate maximum data speeds for different data types.
- Failure monitoring, identify and alert any network component that fails and also test the data circuit from the Internet to the subscriber’s CPE device location when answering support calls.

The access control router that implements the management of pre-pay-on-demand mobile broadband customers has slightly different requirements from the access control router that controls access for fixed broadband customers.

- Provide a captive portal or login page that the customer will use to read the instructions for use and enter the access code that the customer purchased.
- Verify the access code provided by the customer with the access code database that was previously generated.
- When an access code is valid then apply the rate plan rules of maximum download and upload data speeds associated with that access code.
- Initiate a timer to monitor the duration of the access code.
- When the access code duration has expired disconnect the customer from the Internet.

The mobile broadband access control method is also employed in applications where the Internet service is provided without charge, which include hotel guest Internet and retail store WiFi. Hotels may want to give the guest an access code to ensure that only hotel guests have access to the free Internet service.

The following sections describe how the requirements to manage users, customers and subscribers are incorporated into the access control processes.

3.2. Fixed broadband subscriber access control process

The fixed broadband subscriber access control process begins with receiving a data packet from a client via the PtMP wireless access point. The subscriber's CPE is configured with the authentication credential. When the access control router receives the data packet from the PtMP wireless that was received from the CPE the credential is extracted and passed to a process that authenticates the customer. The authentication process consults credential database to verify that the credential is valid. A negative verification means that the access is not permitted and that data packet is discarded. A positive verification identifies the customer and enables access to the Internet. The customer connection passes through two additional processes. The first of these processes uses the customer identification to consult the billing system to verify the customer's payment status; if the account is paid then the process enables the customer's access to the Internet. The second of these processes receives the customer identification and applies the customer rate-plan that was downloaded from the billing system. The rate-plan identifies the maximum download/upload speeds and optionally a data cap for the customer's billing period. The rate-plan for each customer is downloaded to the router when billing system settings change. After authentication the customer is given access to the Internet with the maximum download and upload speeds that were assigned to that customer. The access control router also includes status and failure monitoring.

The access control process is illustrated in the next diagram where each component is identified.

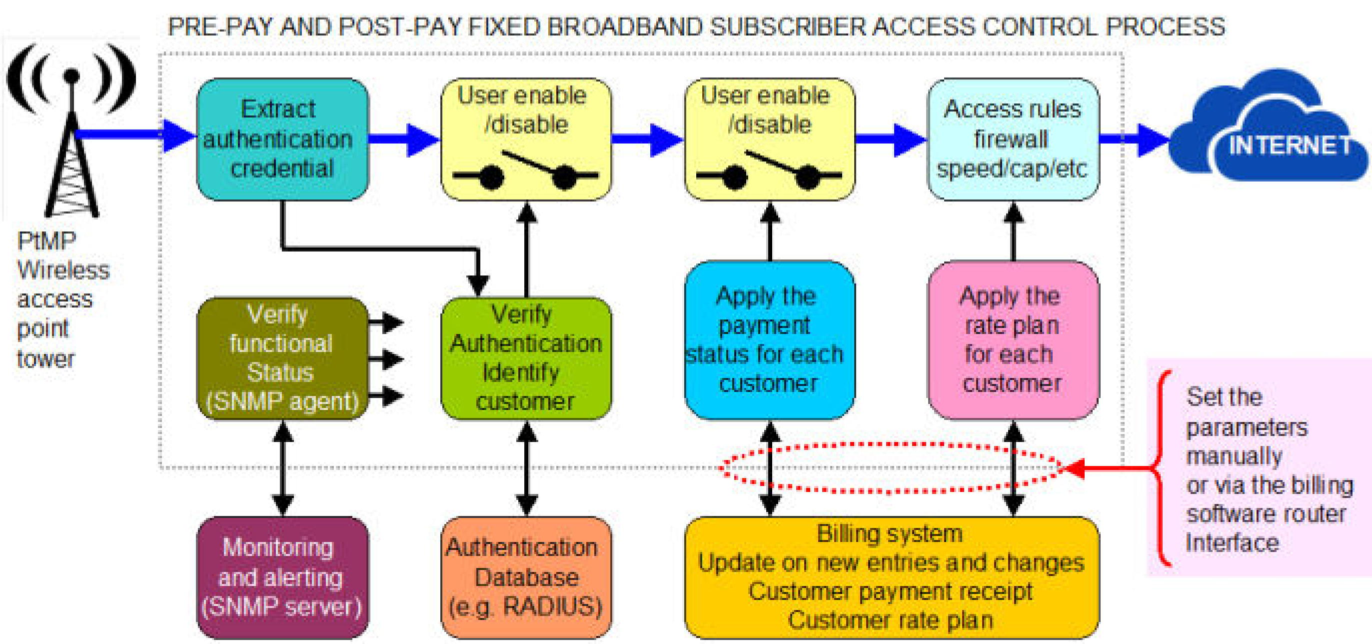


Figure 3.2.1. Fixed broadband access control process for pre-post-pay customers.

3.3. Fixed broadband subscriber authentication methods

The customer authentication process occurs each time that the customer connects to the network in order to verify the customer's identity. A customer is identified when the authentication credential sent by the customers CPE is verified with the customer credential database. The credential is part of the customer record and may be stored as part of a Remote Authentication Dial-In User Service (RADIUS) server database to implement the authentication process. The field service technician configures the customer credential during installation of the CPE at the customer's premises.

Methods of authenticating fixed broadband customers and allowing them onto the network that are commonly employed by WISPs are listed below.

- CPE MAC address verification.
- Point-to-point protocol over Ethernet (PPPoE) using RADIUS authentication.
- WPA2-enterprise using RADIUS authentication.

MAC address verification is the simplest but least secure method of verifying the authenticity of a customer. The MAC address of the customers CPE wireless is added to a table in the access control router either manually or by the provisioning software. When the access control router receives data packets from a customer the MAC address is checked against the MAC address table. When the MAC address is found the data packet is sent forward, if the MAC address is not found the data packet is dropped. With this method it is necessary to incorporate safeguards to verify that an attempt has not been made to duplicate the MAC address in order to hack into the Internet service. The diagram illustrates the data path for MAC authentication.

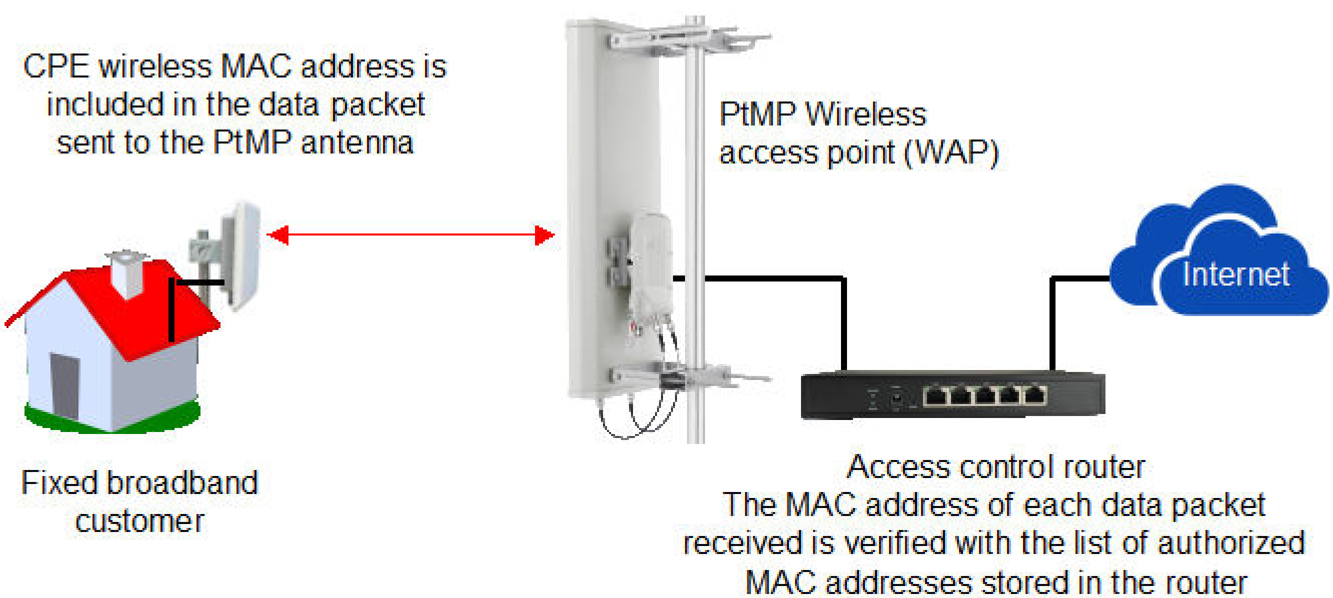


Figure 3.3.1. MAC address authentication of the customer.

Point-to-point protocol over Ethernet (PPPoE) is an authentication method that has been used by DSL service providers for many years and is still popular with WISP's because most programmable routers that are used for access control include a PPPoE service. PPPoE provides authentication, encryption, and compression of the data connection over the data link to the customer, and offers good security for authentication. A PPPoE credential is stored in the CPE wireless and sent to the access control router PPPoE server to initiate a connection. The router PPPoE server authenticates the credential via a Remote Authentication Dial-In User Service (RADIUS) server to allow access to the network. The connection of the access control router with the RADIUS server is shown in the next diagram.

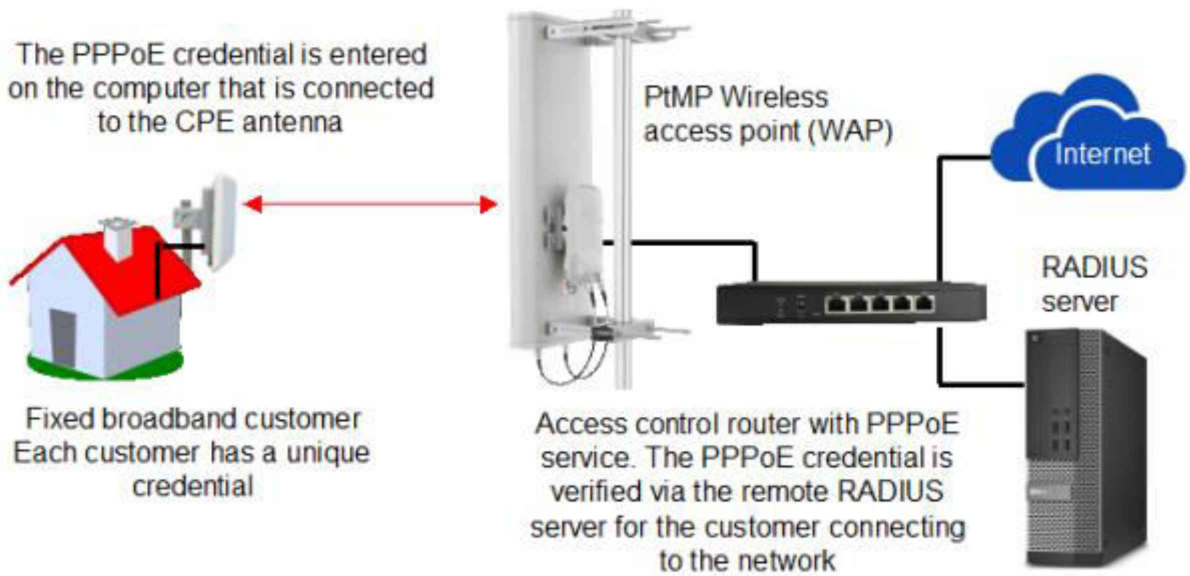


Figure 3.3.2. PPPoE protocol authentication of the customer.

RADIUS authentication is a robust and popular protocol that provides centralized authentication, authorization, and accounting (AAA) management for users who connect and use a network service, ensuring secure access to a network. RADIUS is a client/server protocol and is used in many applications to authorize and control access to a network.

A RADIUS server is also used for WPA2-enterprise authentication. A PtMP wireless with WPA2-enterprise authentication software communicates with the RADIUS server to validate a credential sent by the CPE client. The deployment of WPA2-enterprise authentication in a network requires a WPA2-enterprise client (the CPE wireless) to connect to a WPA2-enterprise server (the PtMP wireless) with a pre-programmed credential sent using the RADIUS protocol. The credential is passed to a RADIUS server for verification. The RADIUS server maintains a database of credentials to permit validation and authorization of many clients.

With WPA2 encryption and authentication each client has the same authentication key, which reduces the security of the method. WPA2-enterprise however requires a unique key for each client, providing greater security. The diagram illustrates the implementation of the network with WPA2-enterprise authentication.

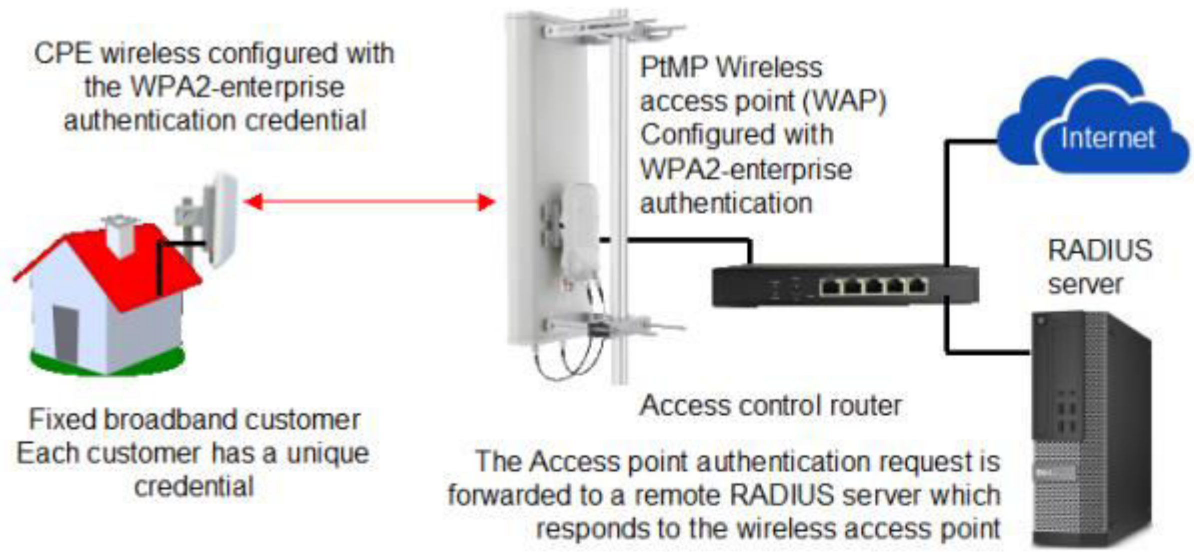


Figure 3.3.3. WPA2-enterprise authentication of the customer using the RADIUS protocol.

3.4. Fixed broadband customer rate plans

An Internet service provider will have several price/performance services to suit the needs of different customers. Each price and performance service is called a rate-plan. Some example rate-plans that a WISP might offer are listed below.

- Plan 1: Maximum data speed, 5Mb/s download, 1 Mb/s upload, cost $10/month.
- Plan 2: Maximum data speed, 10Mb/s download, 2 Mb/s upload, cost $15/month.
- Plan 3: Maximum data speed, 20Mb/s download, 4 Mb/s upload, cost $25/month.
- Plan 4: Maximum data speed, 40Mb/s download, 8 Mb/s upload, cost $45/month.

The customer selects a rate plan when becoming a subscriber. The customer's decision might be based on lowest cost or the need to have fast Internet access. The customer is able to change the rate plan at any time. When a customer has been authorized through the access controller authentication step then the rate plan download and upload data speed limits for that customer are applied to the data connection. The customer then has the maximum data speeds that are specified by the rate-plan agreement. One access control router will control the data speeds of multiple customers and each may have different rate plan maximum speed settings.

3.5. Managing fixed broadband pre-post-pay access control

The access control router has four points of interface with the WISP management software. The WISP management software consists of several modules, two of which interface with the access control router.

- Sales, provisioning and activation. This subsystem provides for the data entry of new customer information together with the rate plan that the customer has chosen. The module has three functions (a) issue an installation work order to the field service technician to install the customer site, (b) add the customer information and rate plan to the billing system, (c) issue a credential to the authentication system for use by the access control router.
- Billing subsystem. This subsystem provides the customer activate/deactivate instruction and the rate plan instruction for the access control router. The billing system issues the monthly invoices to customers and receives a notification when the customer's payment has been received. If the payment is not received by the due date then the customer access is deactivated, and reactivated when the payment is received.
- The network configuration, authentication and monitoring subsystem. This subsystem has two points of interface with the access control router. The first is for customer authentication where the router PPPoE host might pass a RADIUS protocol request for authentication by a server. The second point of interface is the monitoring of the router to gather traffic and functional data; this may be implemented with an SNMP manager communicating with the router SNMP agent. The subsystem also has a function to test the circuit through to the customer CPE device for the case where the customer calls and has no Internet service.
- The customer relationship management (CRM) module. This module provides a portal for the customer to access the account status information, view past invoices, optionally pay for the service on-line, and open a customer support ticket.

Most billing management software will not have an interface to program the router API and so the WISP has to program the router manually with the information provided by the billing system. This is not a time consuming task as the subscriber information is added at one time and only changed if the subscriber does not pay and has to be deactivated or changes the rate plan, although it requires a high level of technical skill.

If the WISP owner prefers to avoid the technical issues with programming routers then a WISP billing software can be chosen that will interface with the router API to set the subscriber parameters each time that a subscriber is added to the system.

The diagram shown in the next figure illustrates the WISP management system software modules that provide information for the access control router. Automating the interface between the software and the router will facilitate the expansion of the network and growth of the WISP business.

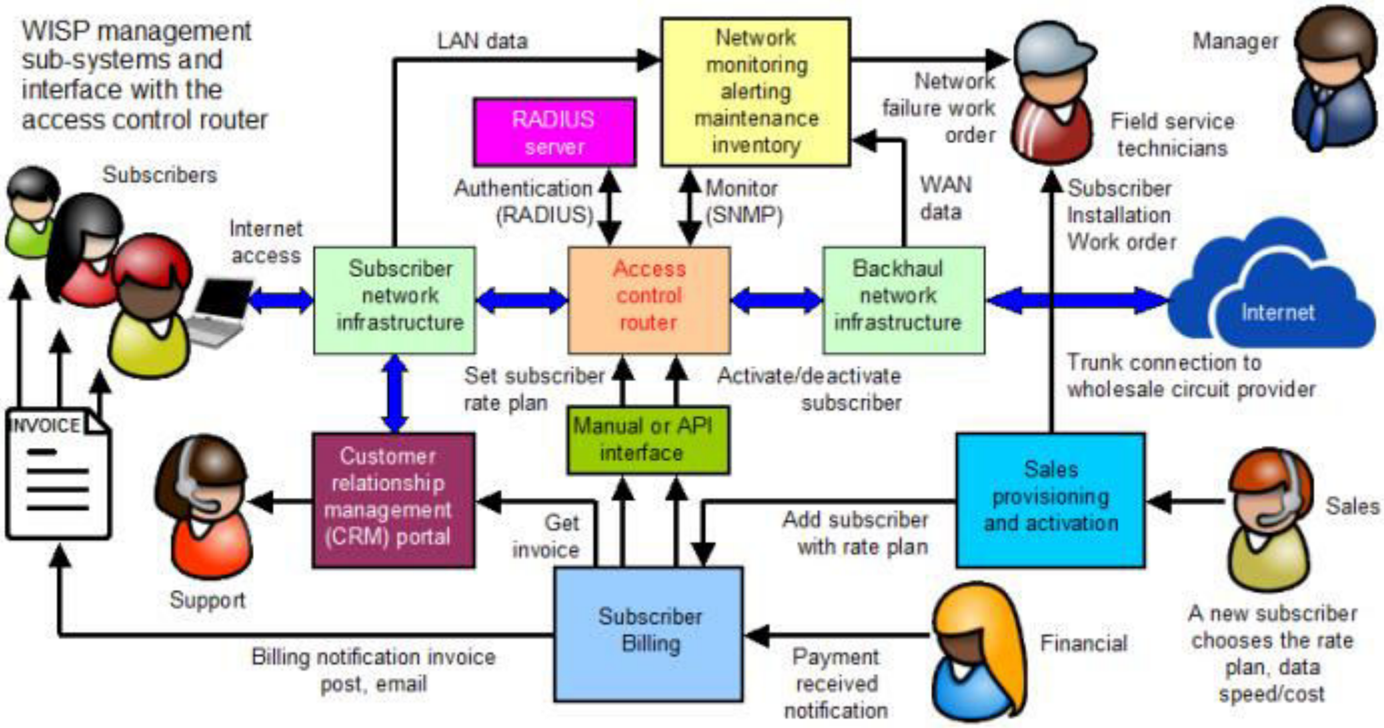


Figure 3.5.1. Fixed broadband access control integration with the WISP management system.

Some cloud management systems for WISP's offer dedicated routers that are integrated with the software to automate the configuration, which will speed the business installation and start-up process, and simplify the business management process. With router automation the WISP owner can facilitate the growth of the business by handing off responsibilities to staff members, as the automated cloud management is simple to use compared with deploying general-purpose programmable routers that require programming by skilled staff.

The WISP has to analyze the trade off between initial costs, on-going operating expenses and the time spent with systems configurations which also has a cost in man-hours with delays to get the service to market. Systems built using open-source software and programmable routers will be less reliable than established and tested cloud systems with integrated access control routers. Reduced reliability and system downtime will represent an additional cost to the WISP, reducing income and customer satisfaction.

3.6. Fixed broadband access control router at the NOC

The access control functionality can be centralized at the NOC or distributed throughout the network and some alternative topologies are elaborated in the following sections to illustrate this point. Four technical solutions, or network topologies, are described for the incorporation of access control in the WISP's network.

The network operations center (NOC) design is a very popular WISP network topology. PtMP wireless towers connect back to the NOC through a wireless distribution network. The NOC then connects to a wholesale network provider through a high capacity circuit. All access control equipment and management software is installed in the NOC.

A router is installed at the NOC to implement access control for all customers. Centralizing the access control function has advantages and disadvantages. The advantage is that all access control is done with one router and so the manual configuration of the router is simplified. It is also easier to interface a software product such as billing with one router to set rate plans and enable/disable customer access to the Internet. However the NOC is a central point of failure and so requires redundant systems that include backup power, duplication of equipment and duplicate Internet connections, which increases the cost of installing the NOC. The centralized design incurs expenses to build out the wireless distribution network as all PtMP towers are connected back to one central location. The diagram of the centralized access control topology is shown in the figure below.

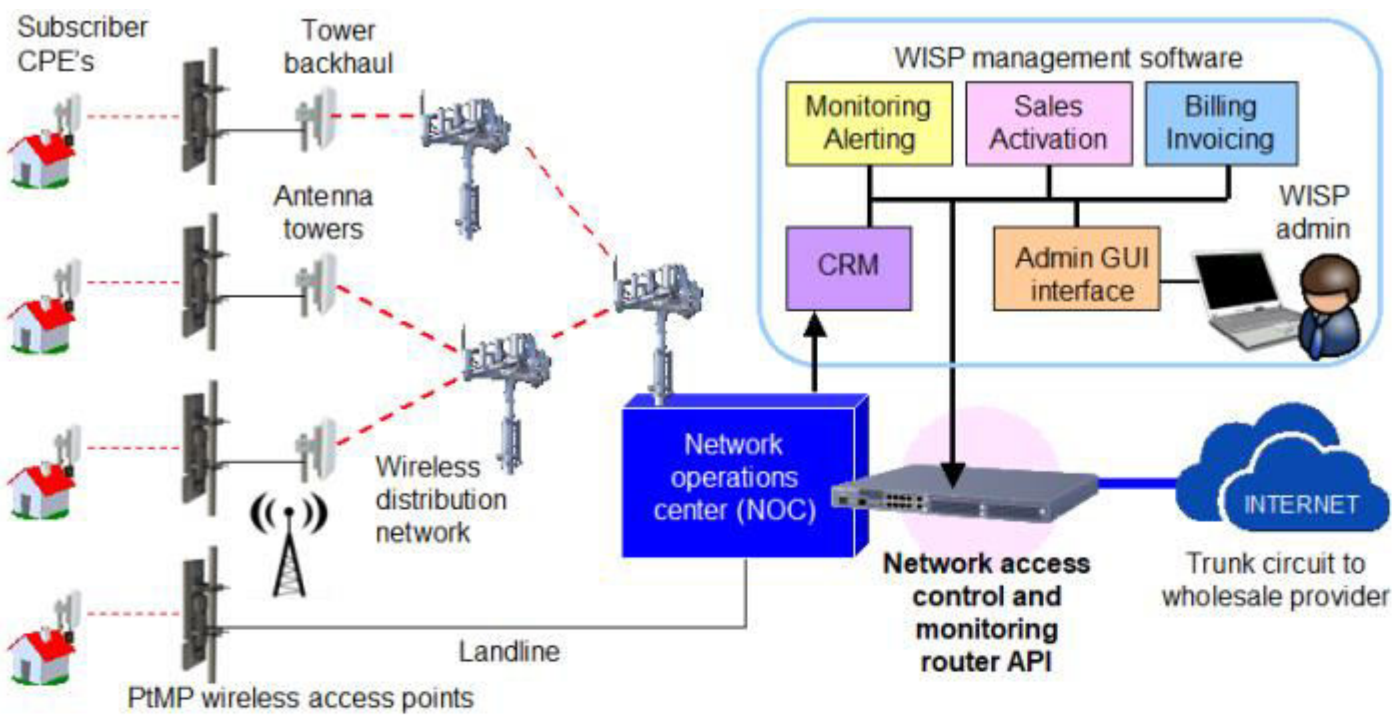


Figure 3.6.1. Access control router installed in the network operations center (NOC).

3.7. Fixed broadband access control router at the tower

A distributed access control topology requires a small access control router to be installed at each tower site. The PtMP wireless connects to the router and then the router connects to the backhaul PtP wireless link, which provides the data connection to the NOC. The router is programmed remotely from the NOC.

The advantage of this topology is that if one access controller fails then only the customers who connect to that tower will be affected. The disadvantage for the WISP who is programming routers manually is that there is now a different router at each tower that has to be configured making the task of router management harder. Each router is configured with only the customers who connect to that tower.

Some cloud management systems support a distributed access control router topology so there is no additional effort when moving from a centralized access control router topology to a distributed router topology. The distributed topology is also much easier to scale than the centralized topology. With the centralized topology the router equipment has to be upgraded for a higher throughput as new towers are added to the network.

An advantage of having an access control router at each tower is that a tower with Internet access, such as a mobile phone tower, does not have to be connected back to the NOC. The distributed access control router topology is illustrated in the figure below.

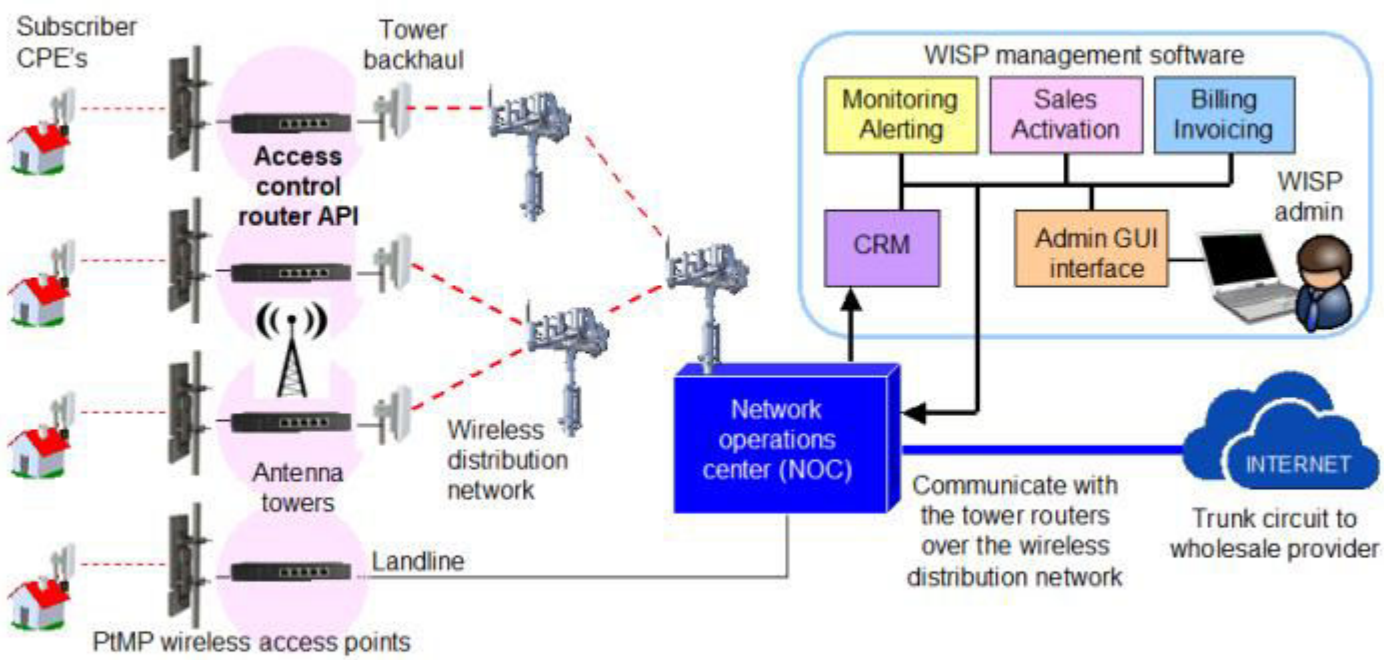


Figure 3.7.1. Access control router installed at each tower site.

3.8. Fixed broadband access control PtMP wireless at the tower

By selecting products from specific manufacturers the access control functionality can be combined with the PtMP wireless access point. The Mikrotik router is very popular with WISP's to implement access control functions and Mikrotik manufacture PtMP wireless products with the RouterOS software. This means that the Mikrotik wireless product can implement both the PtMP wireless access point function and the access control function for the customers that access the PtMP wireless. The PtMP wireless router with access control is programmed exactly like the router installed at each tower. Programming is remote, either manually or automated with the management software. The tower connects back to the NOC via the wireless distribution network, which in turn connects to the wholesale provider WAN. The NOC software connects to the tower equipment via the wireless distribution network using the private subnet IP addresses configured for each access control device. Cloud hosted software may require a port forward rule for every managed device to be installed on a NOC router in order to program individual access control devices. The PtMP wireless can connect to a tower Internet circuit in the case of a mobile phone tower installation.

The figure below illustrates the topology where the PtMP wireless access point is also the access controller for the customers connecting to that PtMP wireless unit. This topology is economical and more reliable with fewer products to malfunction. Programming multiple access control devices will require planning if done manually, and automation of the configuration process will require management software that has been developed for distributed applications.

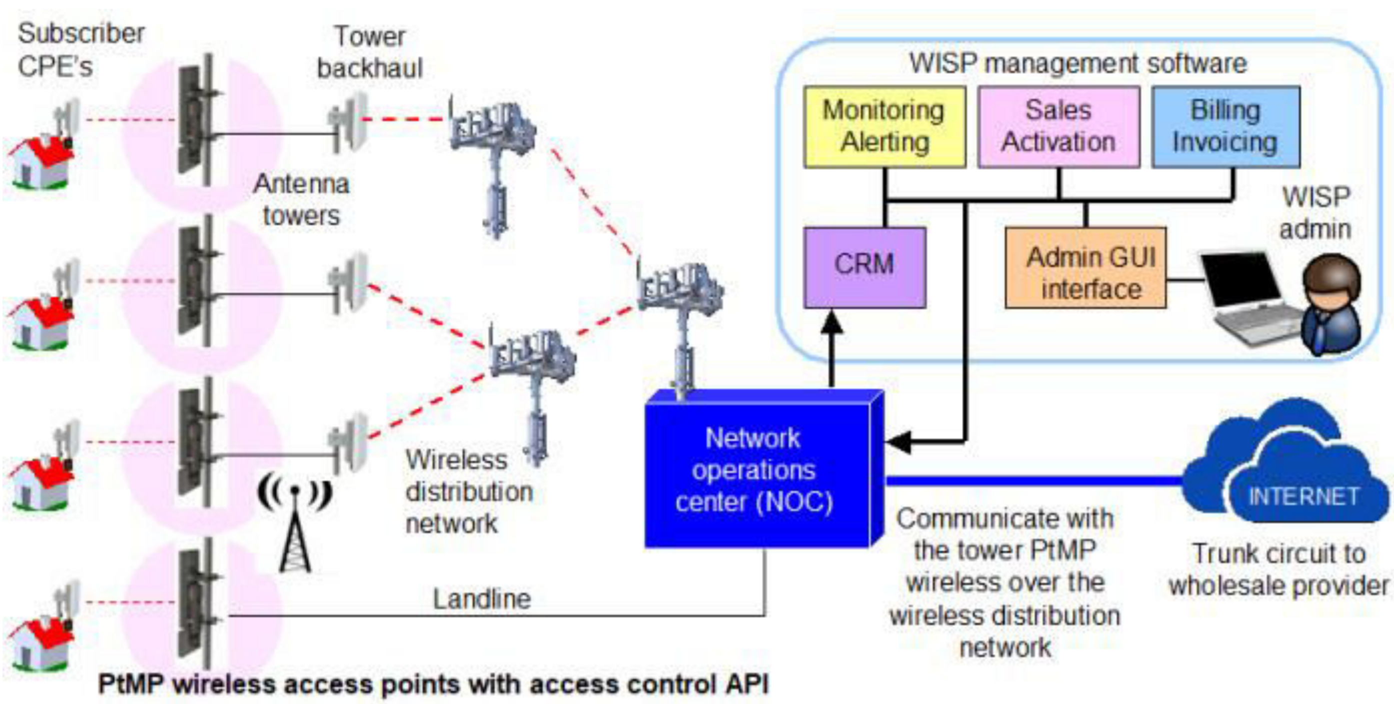


Figure 3.8.1. Access control software installed in the PtMP wireless access point located at each tower site.

3.9. Fixed broadband access control CPE at the client premises

The access control functionality can be added to the CPE if the product has a programmable router capability. The network product company Mikrotik manufactures CPE wireless units with router software. Configuring the access control functionality in the CPE requires communicating with each CPE to program it for authentication, provisioning, enable/disable and monitoring. Manual access control will require remote access to each CPE to program it for the customer parameters. WISP management software that has automated programming for multiple access control routers can manage each CPE when the device is added to the network.

If automating the CPE configuration the WISP management software will require port forwarding rules to be added to network routers in order to access the devices remotely. There are some CPE devices manufactured for WISP software management companies that have dedicated access control software that eliminates the need for network router port forwarding by periodically polling the cloud server for instructions.

The diagram below illustrates the network topology where the CPE wireless units are programmed for access control.

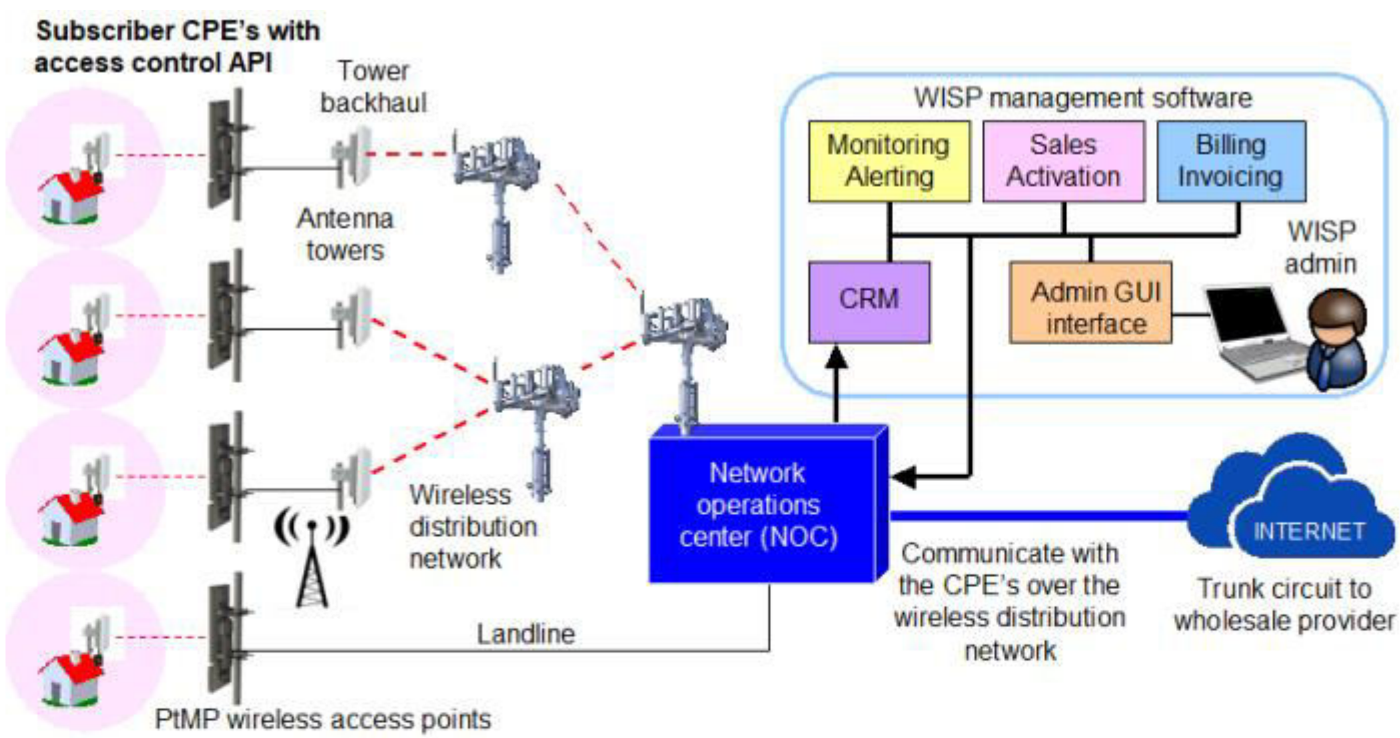


Figure 3.9.1. Access control software installed in the CPE wireless located at each subscriber site.

3.10. Fixed broadband access control at the tower to eliminate the NOC

Most WISPs' choose to implement the NOC based topology, the NOC is the location where the wholesale circuit is installed. As a WISP expands geographically from the central NOC to distances increase between the PtMP towers and the NOC. It will eventually be necessary to build multiple NOC's so that the WISP's network can grow in size. When the access control is located at the tower then the WISP can choose to build a distributed topology, which does not require a NOC. By hosting management software using a cloud service, or else contracting with a cloud management services company and connecting each tower to the nearest point of presence (PoP) the NOC can be eliminated. The WISP can install the PtMP antenna on a tower designed for mobile phone antennas. The tower will probably have a fiber Internet connection with a router that can be configured to provide the bandwidth that the WISP requires If it is not possible to have an Internet connection at the PtMP tower then a PtP link can connect to a tower location where an Internet circuit can be installed, which may be a tall building for example.

A mobile phone tower is a good location to provide Internet access for many prospective clients. The tower will have backup power for high reliability and will have a high bandwidth Internet connection. The tower will also provide environmentally controlled cabinet space to install equipment in a protected environment. A distributed network design topology with the NOC replaced by cloud management software is illustrated in the figure below.

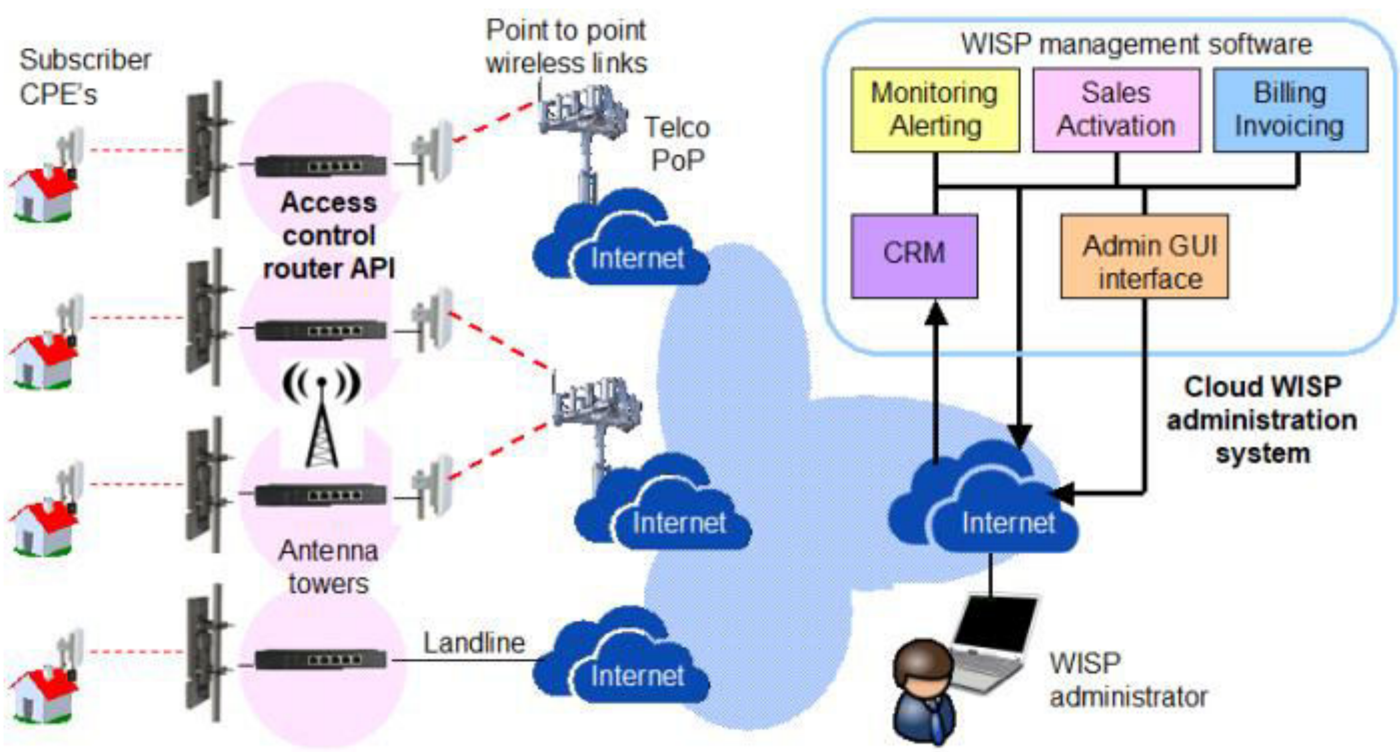


Figure 3.10.1. Distributed network access control topology that eliminates the NOC.

3.11. Fixed broadband access control at the tower with a tower satellite backhaul

A WISP currently has limitations with regard to placement of antenna towers and geographic expansion due to limited locations of wholesale Internet access. WISP's will contract with a wholesale circuit provider to provide a fiber or copper connection at a location that is convenient for the wholesale provider and then the WISP will build a network operations center at that location. The WISP then has to build a wireless point-to-point network out to each PtMP tower. The maximum distance of PtP links, the number of link hops and the terrain are all limiting factors that determine the maximum distance that the WISP can connect a PtMP tower to the NOC. The WISP can only provide an Internet service where a wholesale service is available.

A WISP can contract with a satellite Internet service provider to connect a backhaul via a tower satellite antenna. Currently geo-stationary satellite services are available in some areas of the earth, and low earth orbit (LEO) satellites are beginning to provide a service in some areas of the earth. It is expected that more providers will expand LEO networks significantly to the point where a WISP can contract with a LEO service provider to install an antenna at any point on the surface of the earth. Multiple LEO satellite antennas cannot be installed closely together at the NOC site as they will share one satellite connection, limiting the bandwidth per antenna. However WISP towers are spaced far apart and so a satellite antenna can be installed at each tower. With a satellite antenna on each tower the access control must be installed at the tower using the distributed management topology.

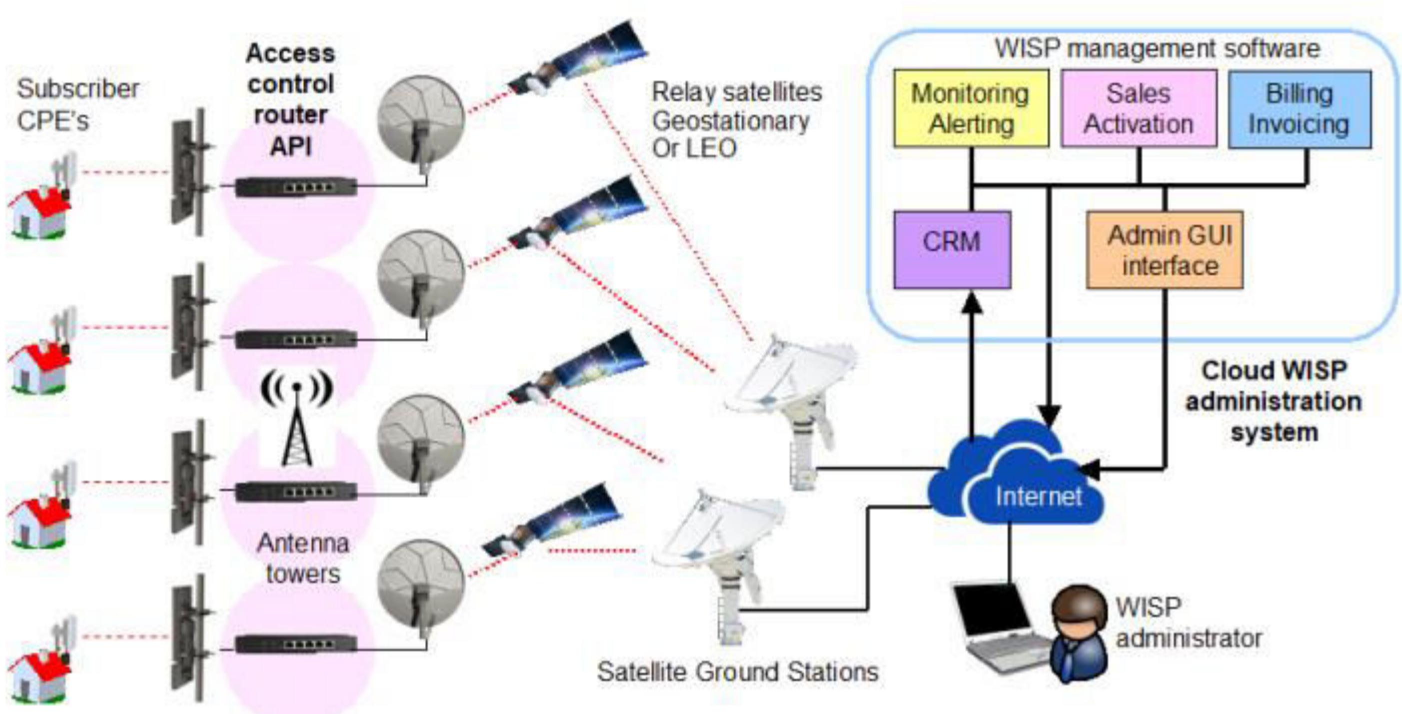


Figure 3.11.1. Distributed network topology with satellite backhauls and access control at each tower.

3.12. Mobile broadband access control for pay-on-demand customers

Pre-pay-on-demand access for mobile broadband requires a different authentication process than that used for the fixed broadband subscriber. In most cases the mobile broadband customer will be anonymous and will connect via an unencrypted PtMP wireless Hotspot. The customer has purchased an access credential either on line or has purchased a voucher, such as a scratch-off card, that has an access code. Unlike the pre-pay or post-pay fixed broadband subscriber who always has an Internet connection, the pre-pay-on-demand customer does not have an Internet connection until the access controller verifies the access code. When the customer connects to the wireless network the access control router captive portal displays a login page in the browser with a box to enter the access code that the customer has purchased. A login page design can also provide the user with an option to purchase an access code on-line using a credit card for payment. The access code will have a fixed duration time and the customer will have Internet access until the access code duration expires.

Most routers can configure a captive portal and authenticate codes with a RADIUS server. Some manufacturers make dedicated access controllers for mobile broadband that have code generation, voucher printing, authentication, activation and payment gateway features in one product. The process diagram shown in the next figure illustrates the on-demand access control data flow.

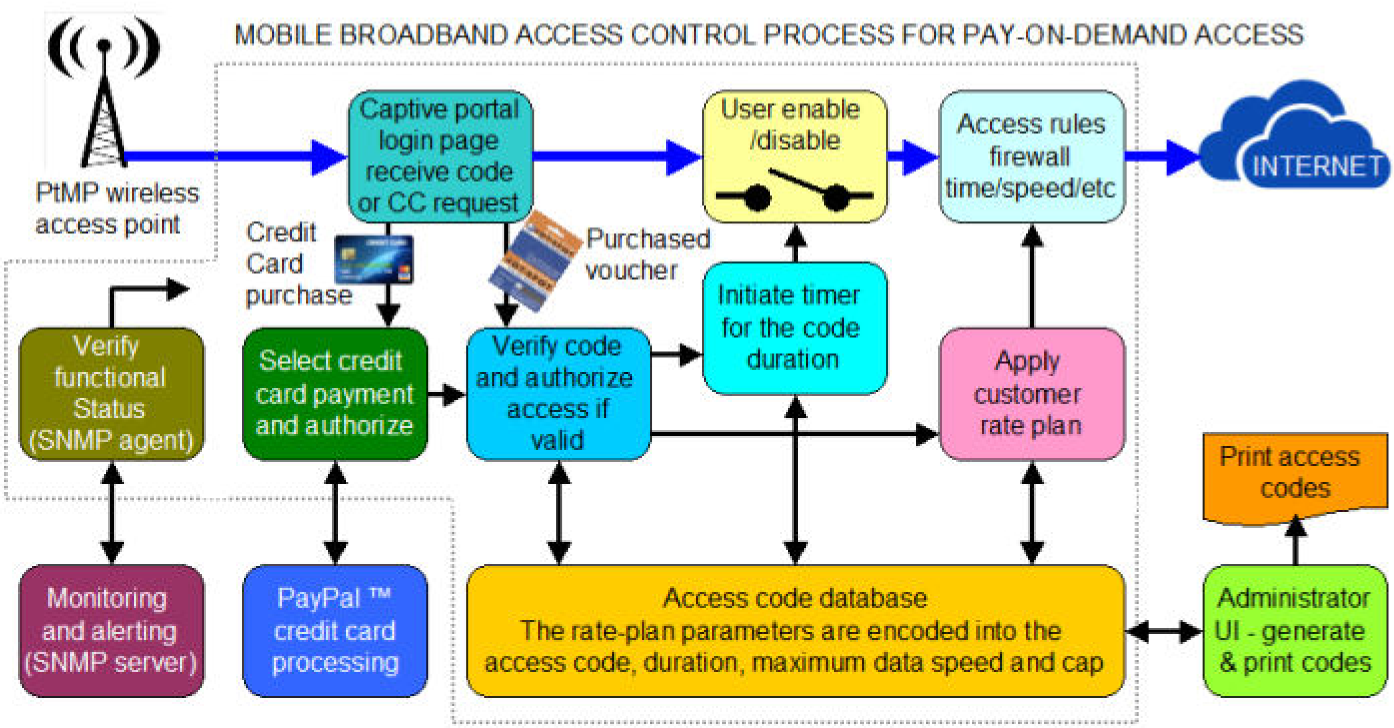


Figure 3.12.1. Mobile broadband access control process for pay-on-demand customers.

The access code is compared with the database of access codes that have been generated and if the code is not found a message is displayed advising no access, and the data packet is discarded. When the code is identified then the customer access to the Internet is enabled for the duration specified, and with speed parameters specified by the code rate plan. The customer has Internet access for the duration specified by the code with the maximum download and upload speed settings and possibly a data cap that the code specified. The access codes are generated by an administrator and printed onto vouchers, or are generated on-demand when the customer purchases codes on-line.

The access control router includes a failure-monitoring component that can alert the administrator if the unit fails, and monitoring can include devices that are connected to the access control unit, such as wireless access points. Several manufacturers package the functionality shown in the figure as a product called an Internet Hotspot gateway. This type of equipment is very popular and is installed in every hotel for guest Internet access, and by many businesses that provide an Internet access service for the public. In some installations the Internet access is free after certain conditions have been met and in others a charge is made for using the Internet. A third type of installation popular with hotels provides free slow speed Internet access but imposes a charge for high speed Internet access.

An example of a captive portal login page and an access code scratch card is shown in the figure below.

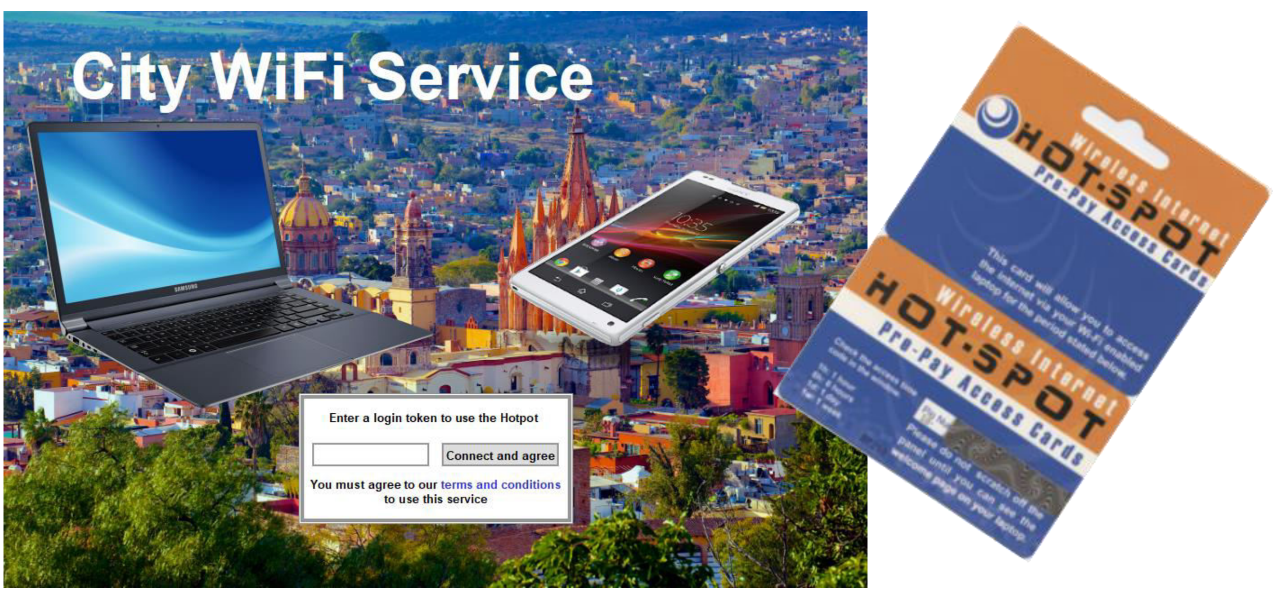


Figure 3.12.2. Pre-pay on demand access control captive portal login page and a pre-payment scratch-off card that has the access code.

3.13. Mobile broadband authentication and customer activation for pay-on-demand

The process of authentication and activation is combined into one step for mobile broadband customers who purchase a pay-on-demand access code and enter the access code into the captive portal. Some fixed broadband customers may also choose to pay-on-demand by purchasing access codes as an alternative to monthly payments.

Pay-on-demand methods are used to sell the Internet service to anonymous mobile Internet users who wish to access the Internet. The pay-on-demand process does not connect the customer to the Internet permanently like a monthly subscription does. Instead the pay-on-demand process connects the customer to the Internet for a time specified by the access code that was purchased. The pay-on-demand connection method for public areas is also called a WiFi Internet Hotspot.

The pay-on-demand process requires the user to purchase a credential, which can be an access code generated on-demand when purchased on-line using a credit card, or else an access code that is sold printed onto a voucher and purchased for a cash payment. The access code encodes the duration of access (days, weeks, etc) and also the rate-plan information that includes the download/upload maximum data speeds permitted and any data cap.

When the access codes are generated each will have parameters that determine the type of Internet access provided for the customer. Activation of pay-on-demand customers is always duration or data limited; the access will terminate after the specified time, or when a specified amount of data has been transferred between the customer and the Internet. Examples of the parameters associated with the access code when it is generated are listed below.

- Duration of the code from the time of first use, this can be hours, days or months.
- Optionally set a date at which the code will terminate after first use.
- Maximum download and upload data speeds permitted, this is important to share the limited bandwidth available between many customers.
- Optionally set the maximum download and upload data byte count permitted. Where the Internet service provider is using a geo-stationary satellite backhaul then the satellite provider may charge by the Gbyte of data transferred.
- Maximum number of devices or customers permitted to use the code concurrently, the default is one, but can be several up to unlimited.
- Determine if a customer can use the code with only one device or with several devices sequentially.

A RADIUS server that is connected to the access control router can validate the access code credential. In most WiFi Hotspot gateway products proprietary software is used to generate the access code, validate the access code and apply the rate-plan encoded in the access code.

The next diagram illustrates combined process of authentication and activation.

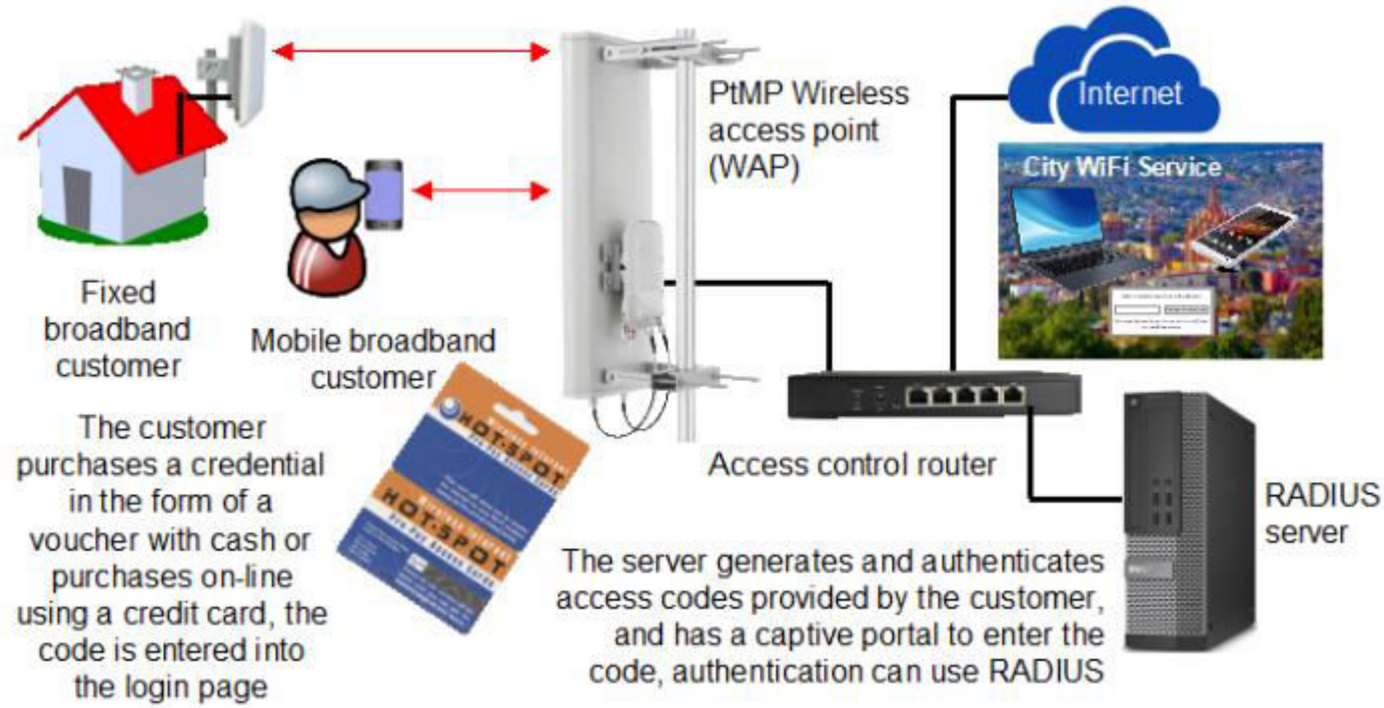


Figure 3.13.1. On-demand authentication and activation of the mobile broadband customer using an access code.

3.14. Methods of selling pay-on-demand access codes for mobile broadband
Mobile broadband Internet access is sold to customers by printing an access code onto a voucher in one of various formats that are then sold through points of sale managed by the service provider. The customer will purchase the access code then enter the code when connecting to the Internet. In many parts of the world people want access to the Internet but don't have credit cards or bank checks to pay for Internet access. Cash payments are used to purchase a code that provides access to the Internet with pre-determined parameters. The code parameters are applied to the data flow in the same way that the rate plan controls data flow for fixed broadband subscribers that pay monthly for the service. Some examples of the methods that the mobile broadband Internet service provider can print and sell access codes are listed below and described in detail on the following pages.

- Print vouchers using a letter printer then cut from 4 x 4 vouchers per sheet.
- Print vouchers using a receipt printer.
- Print scratch-off cards, similar to those used for a lottery.

Mobile broadband access control codes can be sold by printing vouchers using a letter printer. Use the Hotspot gateway software to create access codes with the required parameters then print as a file of vouchers in a 4 x 4 per page format. Send the file to the printer and cut the page into individual vouchers, each with a unique access code. The voucher also shows the duration of the code.

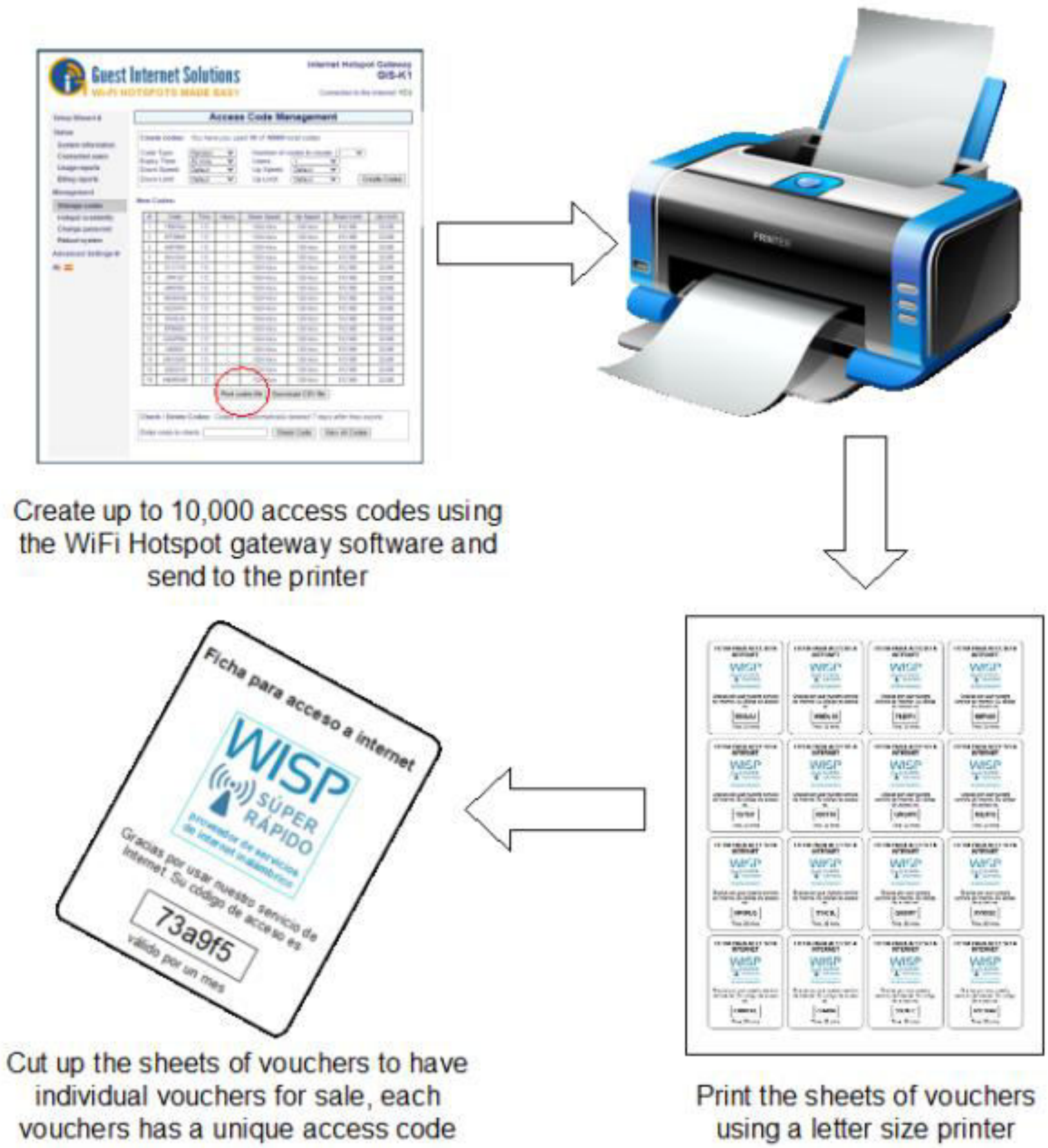


Figure 3.14.1: The process to print vouchers using a letter size printer.

Mobile broadband access control codes can be sold by printing vouchers-on-demand using a receipt printer. Configure the receipt printer software for up to ten different types of access codes. Print a voucher on demand with the parameters requested by the customer. The voucher is sent to the thermal receipt printer and given to the customer. This configuration is popular for an Internet cafe point-of-sale and similar applications.

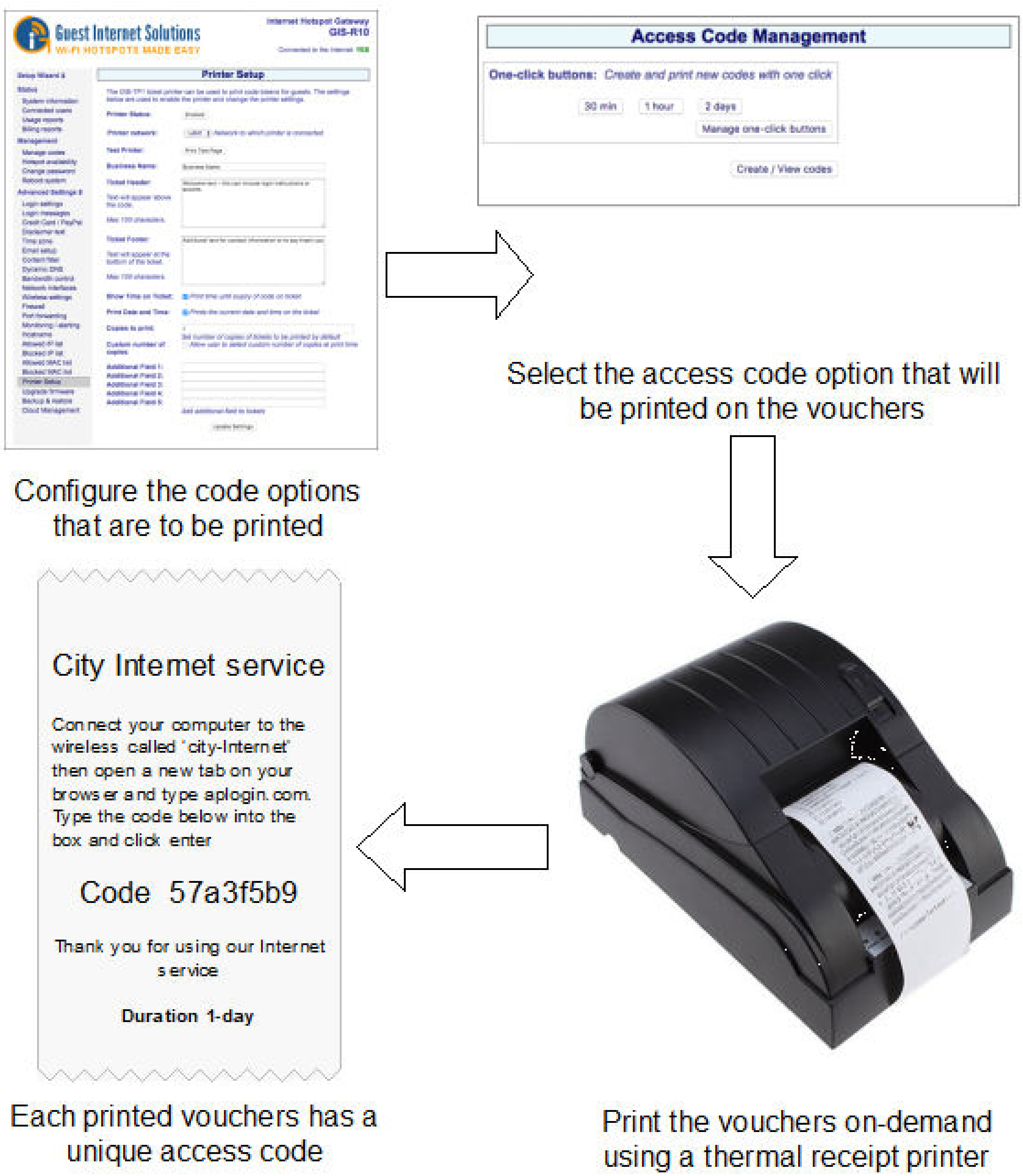


Figure 3.14.2: The process to print vouchers using a thermal receipt printer.

Mobile broadband access control codes can be sold by printing scratch-off cards. Such cards are purchased for phone call minutes. Each card has a unique code that defines the Internet access parameters. A list of codes is generated by the Hotspot gateway software and downloaded as a CSV (comma separated value) file then sent to the printing company via email. Companies print scratch-off cards using special equipment that puts a thin plastic film over the access code. The plastic can be scratched off with the edge of a coin. The Internet service provider will create the scratch-off card artwork. Although the scratch card is more expensive than printing vouchers (10 to 20 cents each) the product gives a professional appearance. The scratch card manufacturer will have a minimum quantity requirement, which may be 1,000 or more cards. The scratch-off card printing process is illustrated in the figure below.

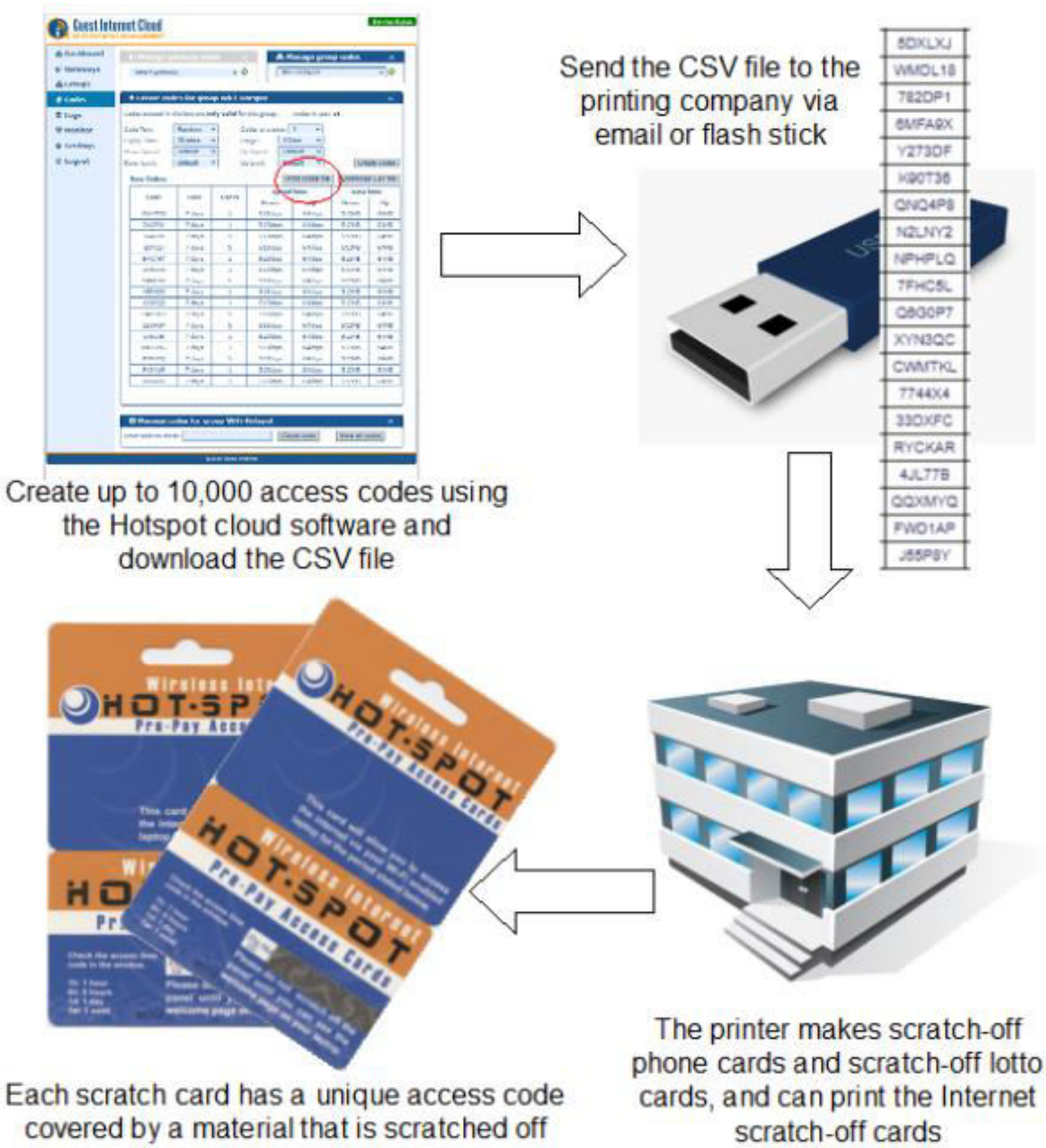


Figure 3.14.3: The process to print scratch-off cards.

3.15. Security concerns with access control for mobile broadband

The fixed broadband wireless connection between the point-to-multipoint wireless access point and the client premise equipment (CPE) wireless uses data encryption (WPA2 or WPA-enterprise). The encrypted wireless connection makes any type of unauthorized access impossible. It is important to keep the WPA2 encryption key secret.

Mobile broadband installations do not use data encryption. If they did then the key would have to be given to everyone making data encryption useless. A mobile broadband Internet service that charges for the Internet access is therefore a target for people who try to hack into the wireless to get free Internet access.

When the wireless connection is not encrypted a hacker can capture wireless transmissions and see the contents of data packets permitting the hacker to see passwords, IP and MAC addresses. Hackers can use a wireless ‘sniffer’ tool to capture wireless data, such as access codes, which is free software that is downloaded from the Internet. ‘Wireshark’ is an example of a ‘Sniffer’ tool.

https://www.wireshark.org/

The ‘Sniffer' software allows a computer to capture data packets that permit the hacker to see IP addresses and MAC addresses of a legitimate user. The hacker can then install the IP address and MAC address of a legitimate user on the hacker’s computer in order to gain free Internet access, a process called ‘spoofing’. The mobile broadband access control must implement measures to prevent hackers getting free Internet access. Some prevention measures are listed below.

- Encrypt login information using SSL to prevent the access code being seen.
- Check MAC addresses for duplications, block any MAC address that is being duplicated.
- Authenticate a customer with both IP and MAC addresses; block any data packet with a different IP or MAC address.
- Generate IP addresses randomly so that the hacker cannot presume that the IP address following the one read is valid.
- Block any attempt to scan ports.

There are occasions when the security measures may conflict with customer device operation. One example is the iPhone operating system, version iOS14 and higher randomizes the device MAC address for security purposes. Apple calls this a 'private address' feature and it is turned on by default. Allowing an iPhone with iOS14 to have access to the mobile broadband service with hacker security protection would require the authentication configuration to be changed to IP only and this would represent a security risk. The iPhone users must therefore be made aware how to disable the 'private address' random MAC feature before using any mobile broadband service.

3.16. Characteristics of routers used for access control

Access control uses a data router and two types of routers are available for deployment by WISP’s for the access control function, as follows.

- A general-purpose router that is programmed using scripts to control the network access of customers. Although general-purpose routers are inexpensive their functionality is limited and automation is difficult to implement which means that most of the routers in use are programmed manually by WISP businesses. It is easy to make programming mistakes and cause a problem with a customer’s service. It is also difficult to scale the business growth, as skilled technicians are required to make router configuration changes and be on call 24/7 in case of network problems.
- A dedicated access control router that has software or firmware written specifically for network access control of customers. Although the dedicated access control router is more expensive than the programmable router the performance and functionality is much greater than a general-purpose router because the software and hardware has been optimized for that purpose. Higher performance includes increased throughput and an increase in the number of customers that can be added to the network. Dedicated access control routers are manufactured by businesses that offer management software and cloud management services for WISP’s because the dedicated access control product can be programmed to interface with the software or cloud interfaces directly to automate the process of configuring the dedicated access controller for customers.

A general-purpose programmable router is often selected for the access control application where the WISP will configure the router manually, or much less frequently, may install management automation software that has an interface for a popular router. Two well-known manufacturers of router products are Cisco and Mikrotik. The majority of WISP’s purchase Mikrotik products due to their low cost and reliable performance. The router has several Ethernet ports and has data packet routing and filtering software that is controlled by pre-programmed instructions. The Mikrotik software is called RouterOS. The router software has a catalog of features that are used to configure hardware ports and also manipulate the data packets that move between the ports of the router. The router is usually configured with one or more WAN ports that connect to the Internet, and one or more LAN ports that the wireless distribution networks and PtMP wireless access points are connected to. As data packets move between the LAN and WAN ports instructions determine what type of processing is done with the data packets. The router can have a series of command line instructions loaded into the memory that determines how the router will process data packets. The sequences of instructions that are loaded into the router are called scripts. The router also has a graphic user interface (GUI), which permits the operator to configure router actions through adding information to tables. The router features include an application-programming interface (API), which permits a remote console or remote software to send instructions to the router. The router software will have a series of special purpose software modules that are designed for specific applications; examples are listed below.

- SNMP agent to permit an SNMP manager to monitor the performance of the router.
- PPPoE host to authenticate CPE clients onto the network using an external RADIUS server.
- DHCP service to issue IP addresses for devices in the LAN subnet.
- A captive portal that may use an external RADIUS server to authenticate access codes.

Mikrotik routers permit the configuration of either the PPPoE host or the captive portal. Both cannot be configured at the same time.

The general-purpose programmable router has command line instructions uploaded to implement the access control tasks.

- Authenticate a customer using one of the methods available; examples are allowed MAC or PPPoE protocol.
- Set the rate plan requirements for each customer, maximum download and upload data speeds, data cap.
- Activate or deactivate the customer's access to the Internet according to the account payment status.
- Status and failure reporting is done using an external monitoring software that interrogates the SNMP client in the router.

The access controller configuration can be programmed manually or via one of the WISP management software or cloud products that will automate the process of configuring access control for each customer by sending instructions to the router API. This will permit the WISP management software to automate the access control functions that are listed below.

- Sales; add a new customer to the router customer list and add the rate plan parameters that the customer has chosen, maximum download and upload data speeds.
- Installation; add the customer authentication credential to permit the customer to access the Internet.
- Billing, activate/deactivate the customer determined by the billing cycle account status.

One drawback of the general-purpose programmable router is that router programming is a skill that requires considerable time to learn; it is not possible to configure routers by programming them with scripts without extensive technical training. The router manufacturers offer the training courses, which have a cost for the WISP. Cisco offers a series of Cisco Certification courses and Mikrotik offers the MUM training courses. A minimum of several months of dedicated study is required to become competent with router configuration. This is an added cost for the WISP owner and will delay the deployment of the WISP network. Alternatively the WISP can hire a trained consultant to configure the routers but as changes are constantly being made to the network this will be an on-going cost.

Dedicated access control routers that are offered by several of the WISP software and cloud management software vendors eliminate the restrictions and expenses that WISP's face when using general purpose routers. The dedicated access control router interfaces with the cloud management software and offers a series of advantages when compared with a general-purpose programmable router, as listed below.

- Performance improvement for equivalent hardware, because the router is used only for specific access control tasks the software can be optimized for a higher level of performance than that of the general-purpose programmable router. A smaller hardware product can be used to achieve the required throughput and client volume then the cost will be lower.
- The WISP cloud management system requires little technical knowledge to install and operate dedicated access control routers, what is called a plug-and-play solution. Dedicated access control routers require no programming as they receive commands via the Internet from software or a cloud service.
- The WISP network deployment is very fast using a WISP cloud management software vendor as the hardware products are plugged together and then the WISP adds the account and client information to the cloud UI to start in business.

The WISP cloud management vendors charge per subscriber which increases the WISP monthly expenses, the charge can range from 10 cents /subscriber /month to $2 /subscriber /month. When a WISP is serving a market in the USA then the WISP cloud charge is not significant as the WISP will be charging the client $50+/month. However in developing markets of the world the client charge and service plan rates are much lower so the WISP can only afford the monthly charge when it is in the range of cents per subscriber per month.

3.17. Additional access control router traffic management features

The primary function of the access control router is to authenticate customers, activate and deactivate customers and apply each customer's rate plan. The router can be programmed for additional functions that may be appropriate for the WISP's requirements to address the needs of customers.

Basic functionality for access control is listed below.

- Forwarding the customers authentication credential to an external RADIUS server, in order to authorize the customers data flow through the access controller.
- Enable or disable the customer data flow based on the billing system advising that the account is paid or not paid.
- Control the maximum download and upload speeds for each customer, corresponding to the rate plan that the customer has chosen.

Some additional traffic management features that the WISP many require are listed below.

- Master bandwidth control, if for some reason the customer rate plan is not manually configured correctly then the router should be configured with a master bandwidth control to prevent any problem with excessive traffic occurring over the network.
- Traffic shaping, configures different type of traffic to flow at different maximum speeds. For example permit email, social media and VoIP services to flow at the maximum permitted speed of the customers rate plan, however video streaming is configured to flow slower than the maximum permitted speed because video streaming requires a constant data flow for a long period of time so uses a lot of bandwidth.
- Configure content filter, a service that customers may require the WISP to provide for parental control or business network management applications. The WISP can contract with a third party service to block web categories, such as social media, adult content or violence.
- Allowed IP list, allows the customer to have access to an IP or domain name while blocked from Internet access. The WISP might desire to permit customers who are blocked from the Internet for non-payment or other reasons to access certain websites. The default allowed website is the CRM portal where the customer can check accounts and make payments.
- Blocked IP list, blocks access to an IP or domain name. The WISP might wish to block access to specific websites for whatever reason. A government might impose censorship restrictions and the WISP has to abide by rules set by the government in order to do business.
- Allowed MAC list, allows a device MAC address to bypass authentication. There are many applications where the WISP may authorize non-subscriber devices access to the Internet. For example the WISP can charge the water or electrical utility to automate meter readings and so electronic meters can be polled and communicate over the WISP’s network to provide meter usage for the utility.
- Blocked MAC list, blocks a device MAC address when attempting authentication. There may be a situation where a customer is abusing the service and is not complying with the terms and conditions. This is especially important for mobile broadband applications.
- Set availability, it may be necessary to shut down the service temporarily for maintenance and so it is desirable to provide a captive portal page to inform customers that maintenance is in progress.

The network administrator will use the following router settings.

- Change the secure administrator password.
- Configure network interfaces, WAN and LAN port settings.
- Configure the captive portal, subscriber messages, hostname and other settings.

- Configure the firewall to block attempts at router hacking.
- Upgrade the router firmware when necessary.
- Backup and restore the router configuration.
- Reboot the router when necessary.

3.18. Summary

The key points or take-a-way's that an entrepreneur should remember when selecting a router product for access control are listed below.

- When analyzing management software, identify the products that offer management of the access control router to automate customer access control, otherwise the router configuration will be a manual process.
- Decide what type of subscribers the WISP business will serve? pre- or post-pay, or on-demand, or all?
- When selecting PtMP wireless equipment and access control routers evaluate the authentication methods that they offer, will the management software support the desired authentication method.
- Evaluate the management software for manual or automated customer activation and deactivation, automate via the billing system if possible so that the customer is deactivated automatically if the payment is not received.
- Determine the billing and service rate plans that will be offered to customers.
- Choose an access control router that permits traffic monitoring and failures via SNMP.
- Evaluate the options between a general-purpose programmable router and a dedicated gateway for access control. The choice of management system will determine this decision.
- There are four alternatives for access control placement in the network architecture, understand how access control fits into the planned network design. The final choice will depend on the management software and the backhaul infrastructure.

4. WISP network design

4.1. WISP network installation planning

When planning the installation of new businesses WISP entrepreneurs generally follow a centralized network design, first building a network operations center (NOC), where the wholesale Internet connection and network management equipment is installed. The NOC is connected to PtMP towers with point-to-point wireless links, and the PtMP towers provide a wireless connection for the customer CPE units.

Once the network operations center has been built and tested then PtMP towers can be built out and connected back to the NOC. The WISP should take advantage of towers that are already built and lease tower space to begin operations quickly. There are service companies that operate mobile phone antenna towers that are suitable for the installation of WISP antennas. If the WISP has to construct towers then there will be an additional investment and further delays before the business can begin operations. The figure below shows the basic plan of the WISP's network.

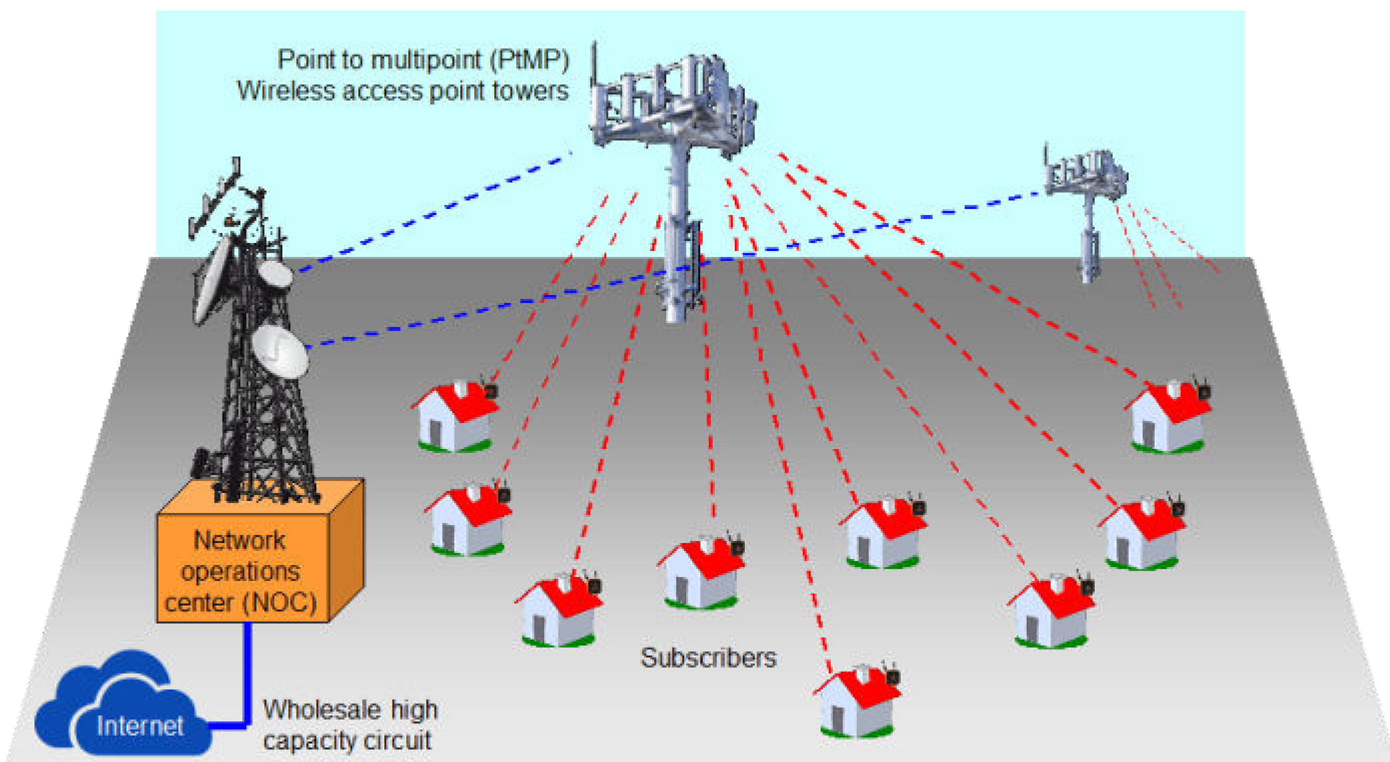


Figure 4.1.1. The WISP business PtMP tower build out.

With the first PtMP tower in place the WISP can begin offering Internet services to prospective customers. The WISP will have calculated a minimum number of subscribers to achieve break-even of business cash flow and so the WISP must push sales quickly to acquire the minimum number of subscribers.

Next the WISP must begin increasing the number of towers to reach the maximum number of subscribers that can be supported by the NOC infrastructure and the capacity of the wholesale circuit to maximize profitability. Once multiple towers have been installed and the capacity of the network operations center and wholesale circuit has been reached then the WISP has to move from growing to a cost optimization mode in order to improve business profits. This will mean making business processes more efficient to handle the workload with less staff. The number of subscriber installations will reduce to maintenance levels with only the replacement of subscribers who have discontinued service.

If the WISP desires to continue expanding then the NOC has to be upgraded with more wholesale circuits. If the NOC capacity is expanded then PtMP towers have to be constructed further from the NOC to expand the area of coverage, which requires more relay/repeaters. A better technical solution may be to build a second NOC close to the new area of coverage.

4.2. Network operation center (NOC)

The NOC design is determined by the following basic requirements.

- The high capacity wholesale network access of Gbit fiber is provided at a location convenient to the wholesaler, the WISP has to set up the business at that location and install the WISP network infrastructure. This location is the Network Operations Center (NOC).
- The WISP has a number of products that have to be installed in the NOC to support the business, the access control router, a server with the WISP management software that includes customer billing, monitoring of the network for failures, sales, provisioning and activation, and software for technical management and configuration of equipment at remote sites. There is also a computer with business software for bookkeeping and payroll.
- The WISP has to carry an inventory of materials that are used by field service technicians so a small warehouse is required. The materials include products to install PtP links, products to install new PtMP towers, and the subscriber installation kits that include the CPE and wireless router. Each field service technician also requires a set of tools and test equipment and so spares have to be kept for losses and breakages.
- The WISP may have a retail store for the public where prospective customers can get information about the Internet service, purchase service plans, and pay bills.

- The WISP will require service vehicles for the technicians to install subscriber CPE wireless units and make repairs to the network so a garaging facility is required.
- An antenna tower must be built for the installation of the PtP antennas that are required to provide wireless links with the remote PtMP antenna towers.
- A backup power generator with electrical storage system is required that can switch over with no loss of voltage to continue operations when the electrical supply fails.
- An air conditioning system with cooling and heating may be required to regulate the temperature and humidity for the computers and network equipment.

The NOC is the weakest link in the network and is a single point of failure; any equipment failure or a power outage without backup will cause all customers to loose Internet access. It is very important to have backup equipment and standby equipment to ensure that the NOC continues to provide subscribers with service. The network operations center infrastructure is shown in the figure below.

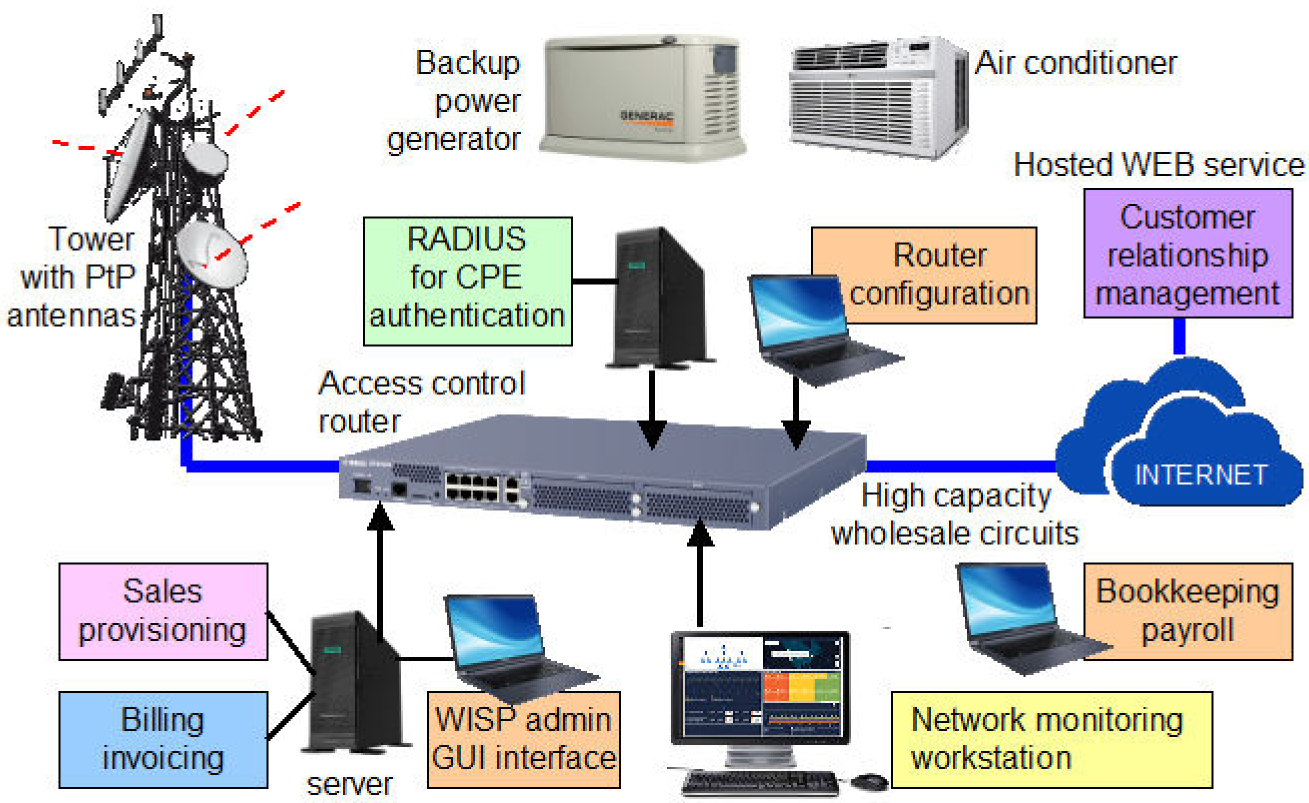


Figure 4.2.1. The network operations center (NOC) infrastructure requirements.

The network operations center represents a considerable investment for the WISP and must be constructed and tested before PtMP towers can be connected via PtP links. This means that WISP has to support operations financially before beginning to generate revenue and see a return on the investment.

4.3. NOC systems integration

In addition to the NOC requirements listed previously there are three further technical steps that have to be determined as part of the NOC design, based on a technical evaluation and the software that is selected to implement the management functions.

- Authentication.
- Automation.
- Monitoring.

An authentication method is required to verify that the customer connecting to the NOC is legitimate, and identify the rate plan that should be applied to that customer. The router that is installed for access control will have several methods available for authentication. The WISP must make a decision about the authentication method before beginning to build out the NOC. There are three popular authentication methods used by WISP’s.

- CPE MAC address authentication.
- Point-to-Point Protocol over Ethernet (PPPoE) authentication.
- WPA2-enterprise authentication.

The MAC address authentication of the CPE device is a simple method. The CPE MAC address is added to the router table to verify the MAC when the CPE communicates over the network. The MAC verification method is simple however it is open to abuse from hackers and so measures to detect MAC address ‘spoofing’ (duplication of a MAC address by another device to get unauthorized Internet access) must be implemented. MAC authentication also requires the wireless distribution system network (WDS) to be configured so that the CPE MAC addresses are transported over the network.

Point-to-Point Protocol over Ethernet (PPPoE) is a popular authentication method used by WISP’s. The router PPPoE interface receives a credential that is programmed into the client CPE device, which then verifies that credential via an external RADIUS service, which stores the authentication credentials for all customers. The RADIUS server credential database is updated from the billing software database, which can store the authentication credential together with the customer record.

WPA2-enterprise is a very secure method of authentication. The CPE device is configured with a unique credential and the PtMP wireless device has a WPA2-enterprise interface, which communicates with the RADIUS server via the radius protocol to authenticate the credential.

Automation refers to the interaction of the WISP management software with the access control router. The access control router has four tasks.

- Identify and authenticate the customer.
- Apply the rate plan selected by the customer, with maximum download and upload speeds, and optional data cap.
- Activate and deactivate the customer according to the billing payment status.
- Monitor the status of the customer's CPE circuit and alert if a failure occurs.

The billing system has the customer authentication credential, the customer rate plan and the customer payment status. The WISP will determine how the billing information is programmed into the router. The WISP can manually install the customer access control parameters in the router using the software commands, or else select billing software that can automate this process through the router API (application program interface). If the WISP chooses to program the router manually then it will be necessary to learn router-programming commands, either through command line programming or else through a router UI that is provided by the router manufacturer. Knowledge of command line programming will be required to manually program the router. The customer identity, rate plan and activation settings have to be configured in the router when done manually. A change is only made to this setting if the customer changes the rate plan, or if the customer does not pay the invoice within the allowed time period in which case the customer is deactivated until the payment is made. The time spent programming the router is small, possibly a few minutes each day. Some billing software and cloud management systems do have an API interface, either for routers that are provided by the software or cloud company, or else for general purpose routers such as those manufactured by Mikrotik. By selecting software or a cloud vendor that supports direct programming of the router the WISP eliminates the need to learn how to program routers and the installation becomes 'plug-and-play. If the WISP has advanced programming skills and a good knowledge of programming routers then an open source software can be chosen that will permit the WISP to code an interface for the router API to automate the configuration process.

The WISP also has to make a decision about the implementation of monitoring for all equipment in the WISP's network in order to gather network performance data and also to detect failures and generate alarms. It is important to have the facility to monitor the circuit out to the CPE and generate an alarm if the CPE goes off-line. A feature is also necessary for customer support staff to test the circuit to the CPE for the occasions when the customer calls to advise that the Internet access is not working. Testing the circuit out to the CPE is required to make a decision about proceeding with a repair. The WISP should purchase equipment that incorporates a SNMP agent and install SNMP monitoring software that can communicate with all SNMP devices. Some WISP management software and cloud management systems incorporate network monitoring. It may be the case that WISP management software provided by a hardware manufacturer can only monitor the products that are manufactured by that company. If the WISP decides to use software provided by a product manufacturer then additional monitoring software will probably be required for devices with SNMP agents to ensure that the WISP has comprehensive network monitoring. In addition to testing subscriber circuits, monitoring is essential to measure data traffic over point-to-point links in order to assess if the link is near to maximum capacity or if the maximum capacity is being exceeded. The result of exceeding the link capacity is that the customer Internet speed will drop below the maximum speed that the customer contracted. The transmission delay time for Internet access, called latency, will increase. When a link is detected near or exceeding maximum data capacity then that link should be upgraded to a faster data speed.

From a business point of view the WISP is installing equipment that will generate an income, providing of course that the equipment continues functioning. Equipment downtime is the time that the equipment is not working and therefore no income is generated during downtime and the customer will want a refund. Minimize downtime by monitoring all equipments for failure and alert technical staff immediately when any equipment fails. The monitoring software may have a feature to send an email or text message to the field service technician with a work order that has instructions for the repair so that the repair can be made as quickly as possible. If the monitoring software does not have a messaging feature then an application program designed for messaging might add this feature.

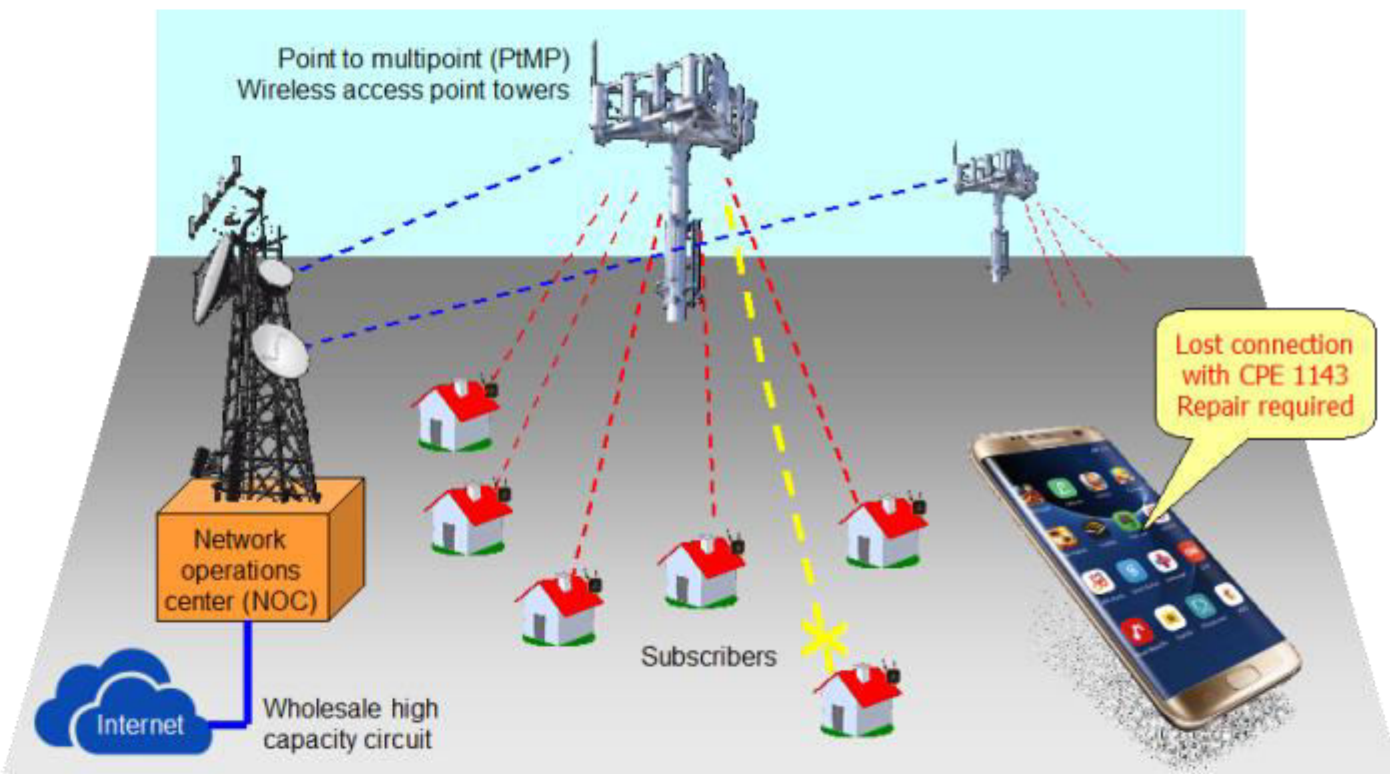


Figure 4.3.1. WISP monitoring alert automation.

A WISP entrepreneur with limited technical knowledge is advised to work with a cloud management system provider, especially if that vendor has an interface for a router provided by the vendor, or for a popular router such as those manufactured by Mikrotik. Most cloud vendors charge between $1 to $2 per subscriber per month and while this might be a reasonable charge for WISP’s in the USA it is too high for WISPs in developing economies where the WISP might charge a subscriber between $1 to $5 per month for a low speed service. Fortunately there are a few providers who charge much less, in the range of 10 cents per subscriber per month, which is compatible with the economic situation in emerging economies. WISP management system vendors are listed in the references at the end of this book. The following diagram illustrates the NOC configuration when using a cloud vendor to provide the management systems.

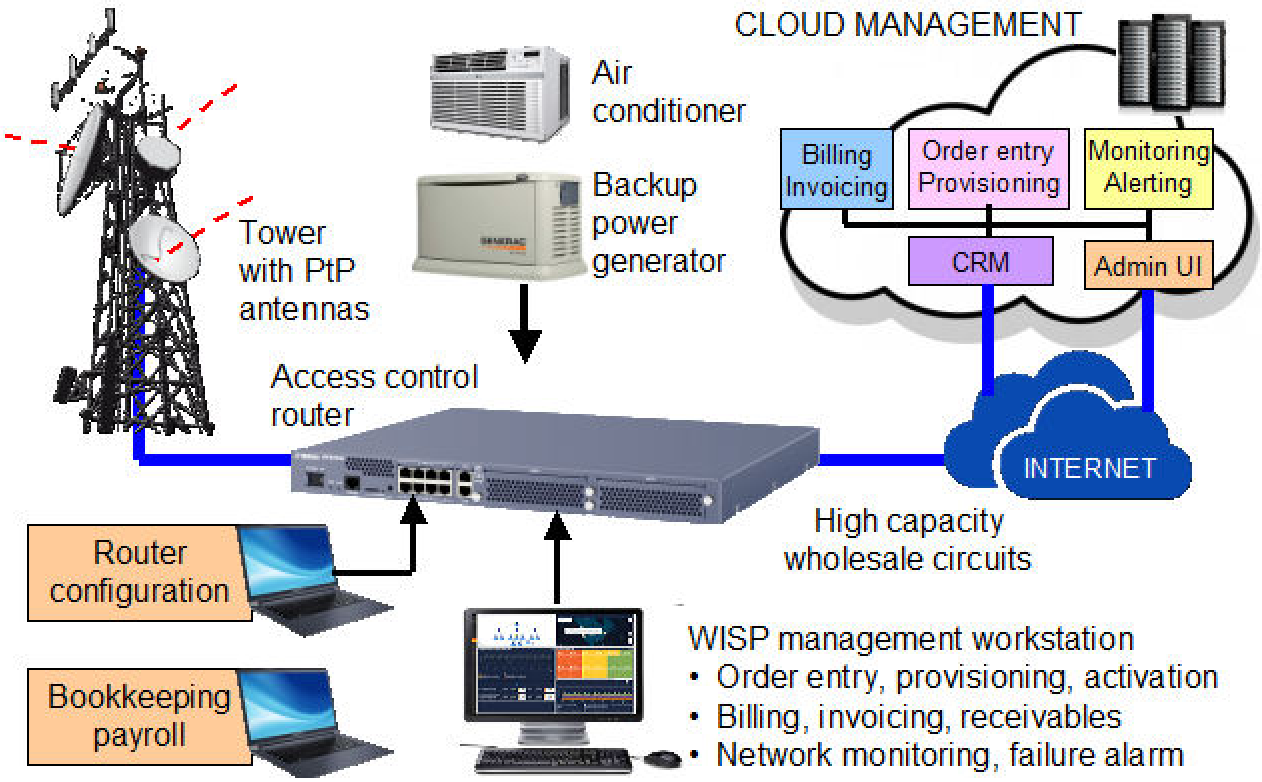


Figure 4.3.2. WISP systems automation via a cloud vendor.

The decisions about selecting the authentication, automation and monitoring methods are partly determined by the equipment and software that is purchased by the WISP. The decision for each of these hardware and software products requires technical analysis and so the WISP who has limited technical knowledge is advised to seek the advice of other WISP's and possibly copy a solution that another WISP has installed and is working successfully. Vendors will only provide technical support for their products and so the WISP must rely on other WISP's for advice and support, especially someone who is starting a WISP business with limited experience. Contact with other WISP's can be facilitated through trade organizations and social media groups. Some manufacturers such as Ubiquiti and Mikrotik also have user groups where a WISP can seek advice from other users. A list of organizations and manufacturers is provided in the reference list at the end of this book.

4.4. Locating the point to multi-point antenna

While the NOC installation is in progress the WISP can identify the first site to install the PtMP antenna and PtP backhaul to the NOC. The first step is to identify where the target customers are located. The WISP will also decide if the target customers are residences or businesses as it is likely that these two groups are in different areas. Eventually more PtMP antennas will be installed to provide coverage for different groups of customers.

The WISP might identify several locations that have a large group of potential customers. Depending on the backhaul speed from the PtMP tower to the NOC and the performance of the wireless products installed at the tower, the number of customers that are targeted for connection at that tower might lie between 50 and 300, with customer capacity determined mainly by the backhaul data speed. Several factors will influence the decision.

- The ease of selling to prospective customers quickly to reach the break-even income for the installation.
- Assessment the financial ability of the target customers to ensure that people can afford the cost of the Internet service.
- Evaluate the area to find a suitable location to install the PtMP antenna to get maximum coverage and ensure a large number of potential customers.
- Evaluate the facility to install the backhaul PtP connection to the NOC.
- Calculate the cost of installation plus ongoing fees such as site rental, which will raise the break-even revenue that must be achieved.
- Evaluate the competitive situation around the PtMP site, is there an ISP offering a DSL service? Is there another WISP who can also offer a similar service in that area?
- If there are competitors what do they charge for Internet service, can the new WISP service undercut their prices?
- What facilities are there to market the Internet service to prospective customers, for example is it possible to have a door-to-door flyer campaign?

Once the WISP has identified the desired area of coverage that has the largest potential group of customers then the WISP must find a high point to install the PtMP antenna that can give the largest amount of people line-of-sight (LOS) to the antenna. The WISP can consult survey contour maps that show the terrain height.

The WISP can choose one of four options to install the PtMP antenna.

- On the roof of a tall building.
- On an existing antenna tower, for example a tower used by mobile phone carriers.
- Build an antenna tower to install the PtMP antenna.
- Use a natural geographic location, for example a hill overlooking a town.

The options will change when considering a PtMP antenna installation in an urban area vs. a rural area. For example, a rural location will not have a tall building or an existing tower. The sections that follow present installation solutions for urban and rural areas.

4.5. Point to multi-point installations in urban areas

Installation of a PtMP antenna in an urban area can usually be accomplished by installing the antenna on the roof of a tall building. This approach is taken by mobile phone carriers when seeking urban locations to install their antennas. It is customary for the building owner to seek a rental fee for use of the roof space. The mobile phone carrier will also need a room at the top of the building to install wireless equipment and backup power so the building owner will charge the mobile phone company a high fee. The WISP antenna installation has an advantage that the volume of equipment is small and can be installed in a box at the base of the antenna so the fee should be correspondingly smaller.

There are two advantages when installing the antenna on the roof of a tall building.

- The building has electrical power available although the WISP should install a battery backup in care of a power outage.
- It should be possible to get an Internet connection to the building, possibly a fast DSL or fiber connection, however ensure that that the provider allows the service to be resold.

The WISP should follow all building code requirements for compliance with the law and also comply with the insurance requirements of the building. This includes the following.

- Get building permits for the installation and have the installation inspected when complete; this will require licensed contractors to work on the installation that may include civil engineer, mechanical engineer and low-voltage technician.
- Follow the local building code rules, install a lightening conductor, ensure that the antenna pole strength and method of fixing to the roof is adequate for the installation and will resist high winds.
- Obtain liability insurance coverage as required by the building owner or manager.

There will also be additional wiring work in the building when an antenna is installed on the roof. Power will not be available on the building roof so the WISP will either negotiate with the building owner to bring low voltage power to the roof, or else install a solar panel with battery and power supply to power the antenna. If low voltage power is provided on the building roof then a backup battery must be installed. In addition the wholesale circuit provider will deliver the Internet circuit to an equipment room at the base of the building. Most tall buildings have a vertical cable shaft for phone and electrical cables and so the WISP will have to contract services to run a data cable from the ground floor to the roof with the approval of the building owner or manager. The building roof installation is illustrated in the next figure.

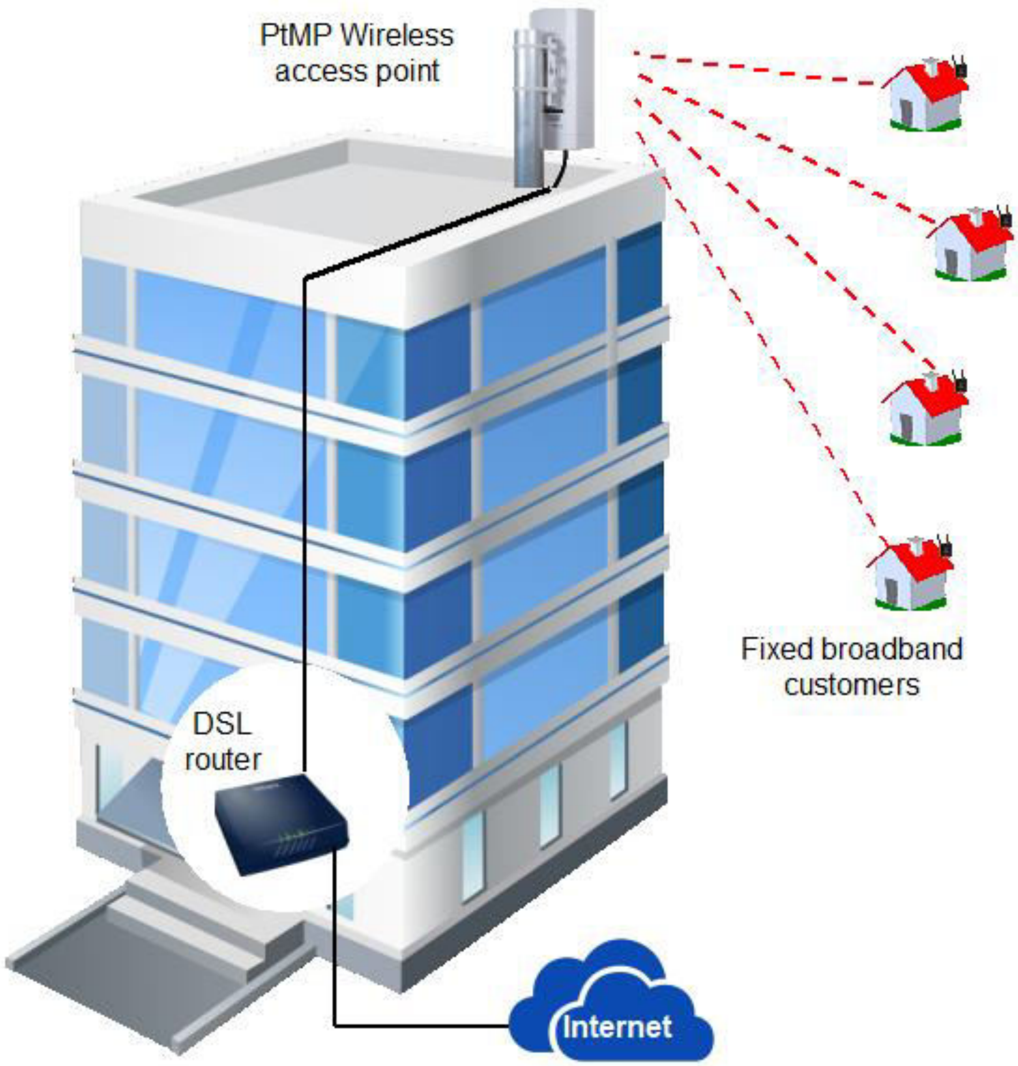


Figure 4.5.1. PtMP wireless access point installed on the roof of a building with an Internet connection to the building.

If an Internet wholesale circuit cannot be installed in the building, or if it is not possible to install the data wiring from the ground floor to the roof, then a point-to-point wireless backhaul can be installed to provide the Internet connection for the PtMP antenna. The building roof will require line-of-site to the NOC antenna tower. If line-of-site is not available then a relay/repeater can be installed at an intermediate point. Roof antenna installations will be subject to high winds and so the installation must be sufficiently robust to withstand the high winds. If the WISP is in doubt about the strength of the installation a mechanical engineer should be consulted. The next figure illustrates a building with a PtMP antenna and a backhaul PtP wireless connection to the NOC.

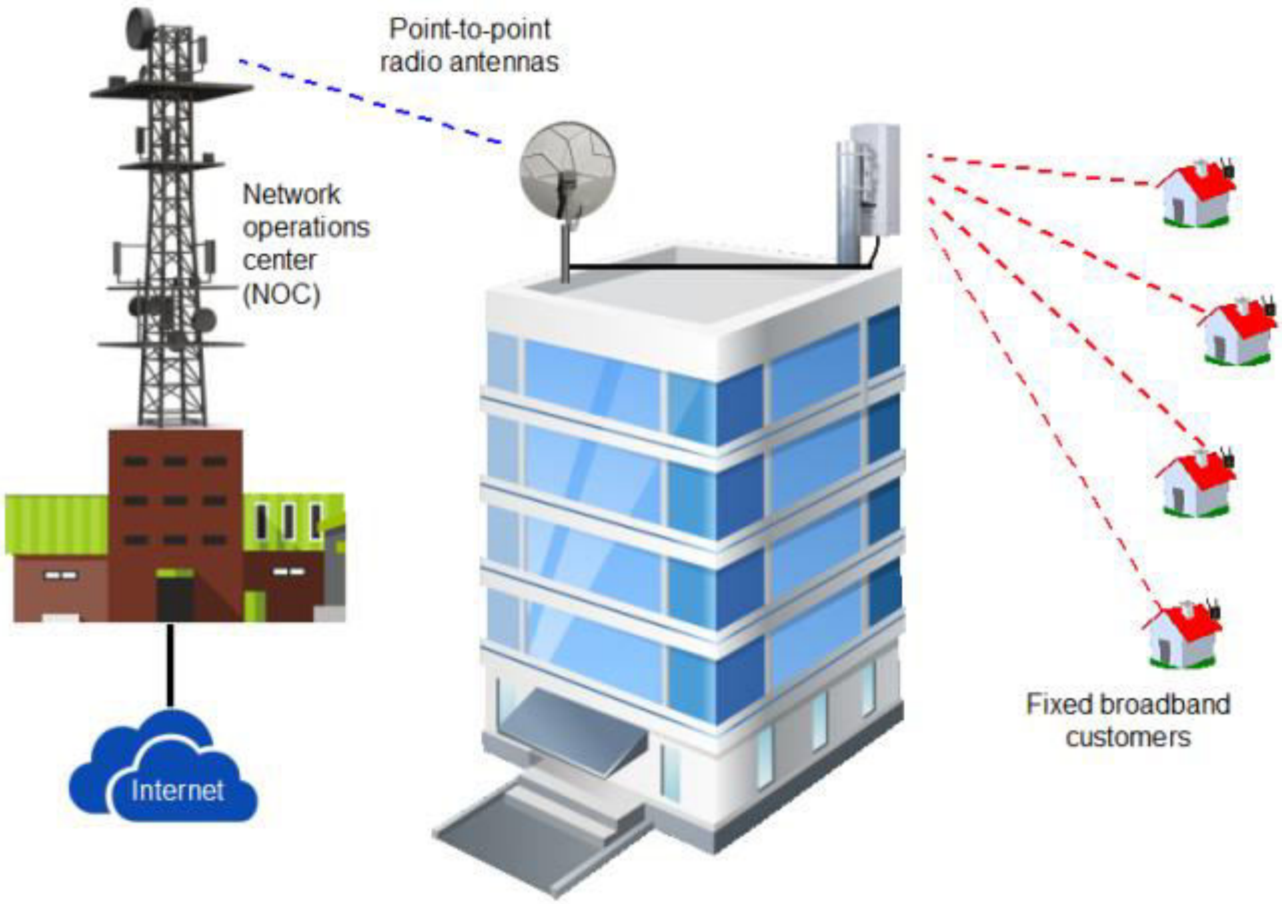


Figure 4.5.2. Roof PtMP antenna with PtP link to the NOC.

The alternative to a tall building in an urban area is to install the PtMP antenna on an existing tower that is being used for mobile phone antennas. In many cases the antenna tower is not owned by the mobile phone company, but was constructed by a specialist tower development company who leases space on the tower to one or more mobile phone companies. The tower will have mounting points for antennas, a facility to run cables down the inside of the tower and an environmentally controlled equipment room or cabinet at the base of the tower. The tower will have electricity with backup power and will have an Internet data connection. The tower lease will be expensive but the location will be excellent and will provide good coverage over the target area. The tower will comply with building code requirements, including lightening conductors. The WISP will not be permitted to install antennas and equipment however; the WISP will pay the tower owners licensed and insured contractors to do the installation work. The WISP will not have access to the equipment once installed and if there is an equipment failure the

WISP will call the tower owner or operator who will send a contractor to replace the equipment that is provided by the WISP. The WISP should always install very robust and reliable equipment on a mobile phone tower, as any repair will take several days to complete. The WISP should also install remotely managed power-monitoring equipment that can power cycle the WISP's equipment to reboot it. A mobile phone tower is an excellent technical solution for the WISP PtMP antenna installation but will be the most expensive option, with high installation costs and high monthly lease charges. The diagram below shows the ISP antenna installation on a mobile phone tower.

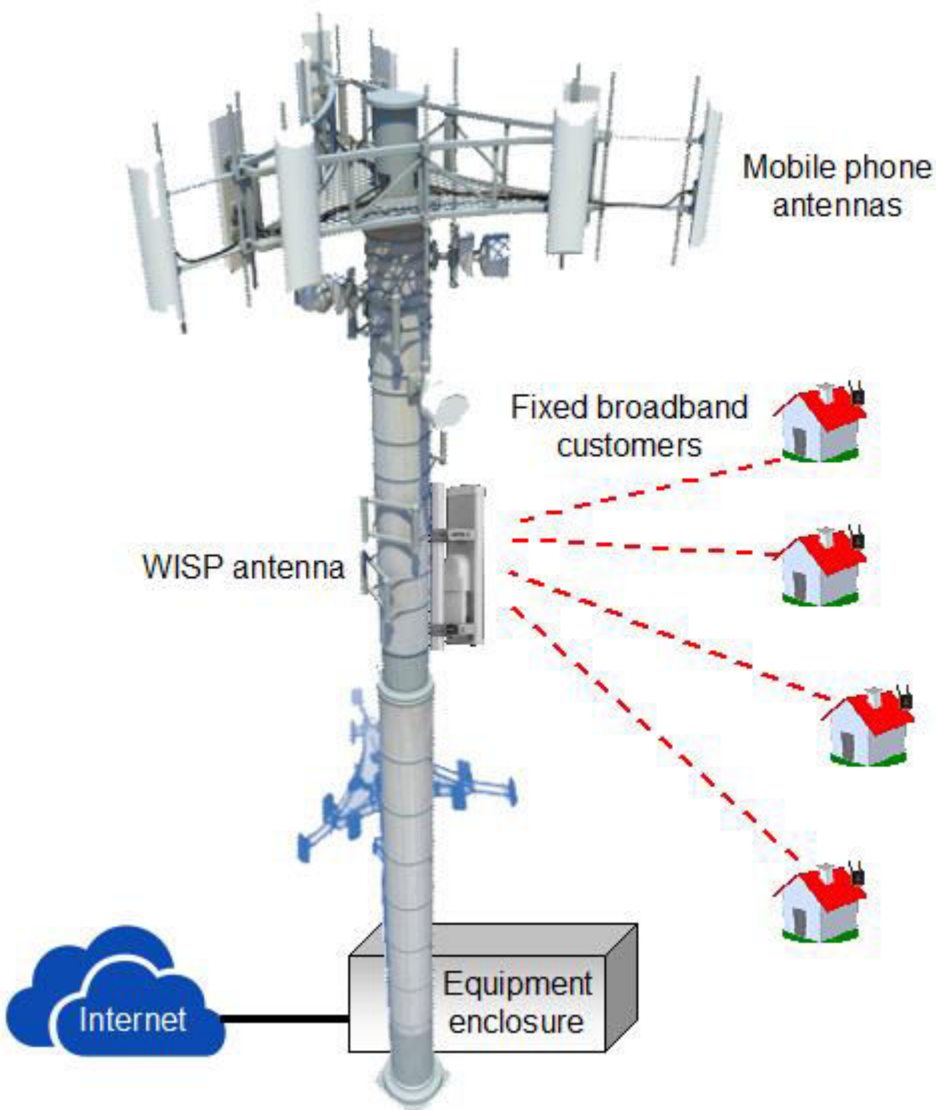


Figure 4.5.3. Mobile phone antenna tower with the WISP PtMP antenna installed.

If the geography has a hill or slope facing the area where customers are located the WISP can install a PtMP antenna with PtP backhaul and solar panel with batteries to power the installation. The target area might be a small town in a valley with the equipment installed on the side of the valley. The WISP will have to negotiate with the land property owner to determine a rental fee to install an antenna on a small area of land. The antenna location must be accessible by a vehicle in order to take the equipment for installation and to maintain the equipment.

The figure below illustrates what such an installation might look like. The PtMP and PtP equipment is installed on the side of the valley overlooking the town. The WISP NOC is located in the town with a parabolic antenna providing the PtP link for the equipment at the side of the valley. The PtMP antenna can provide coverage for the whole town. If the geography of the region permits then this type of installation is the preferred approach to building the network infrastructure.

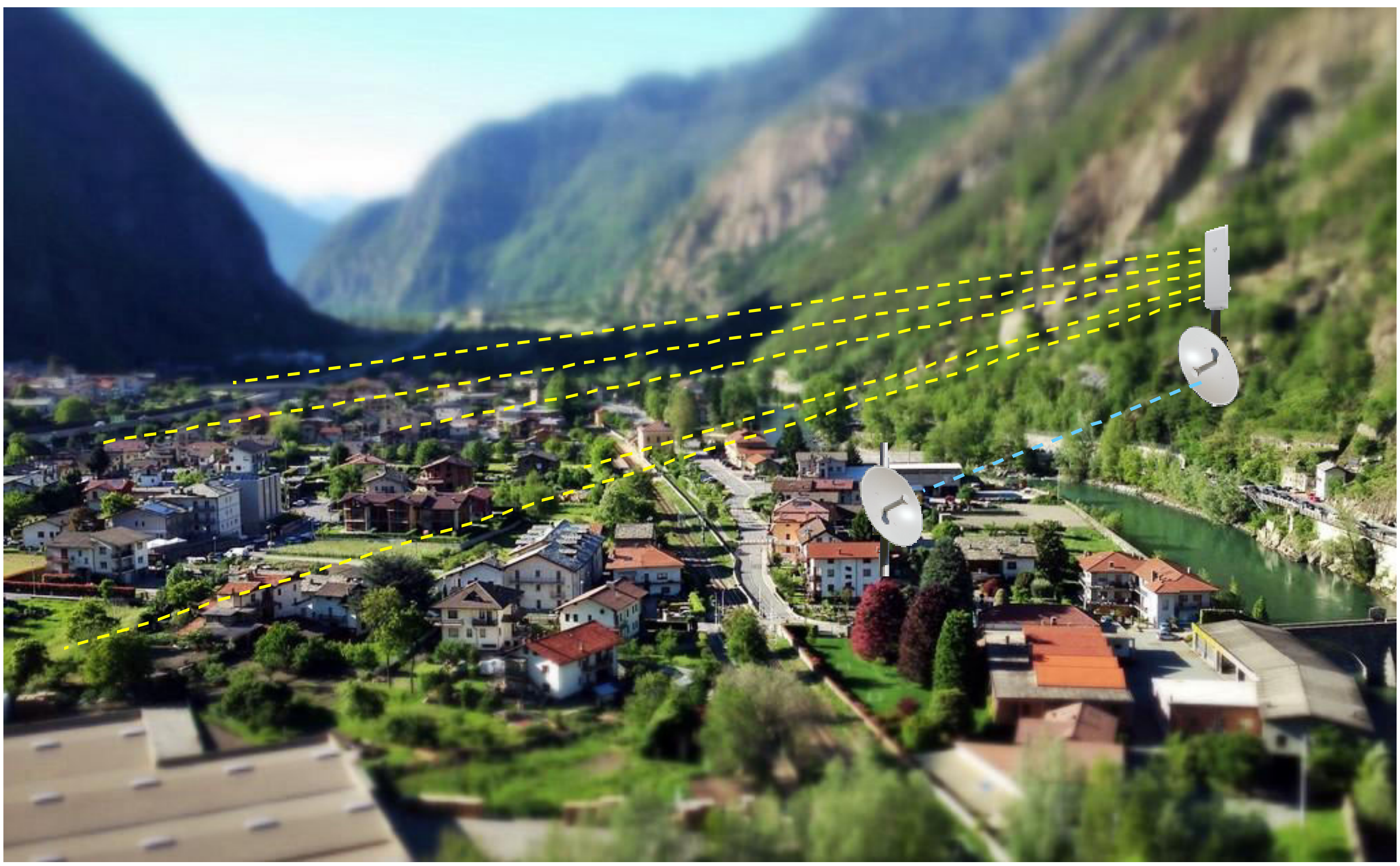


Figure 4.5.4. PtMP wireless access point with backhaul PtP antenna installed on a hillside overlooking the town.

The hillside installation must be robust with a fence around it to protect it from animals. The WISP should install environmental monitoring to measure the conditions of the equipment. The WISP should install an IP camera to observe the installation.

Figure 4.5.5. PtMP wireless access point with backhaul PtP antenna, solar panel and equipment enclosure with batteries, installed on a hillside.

The last of the four PtMP antenna installation alternatives is to construct an antenna tower in an urban area. The option of constructing an antenna tower in an urban area is usually a last resort and some of the reasons why it is difficult to construct an urban area tower are listed below.

- Urban areas do not usually have land available and it is often necessary to purchase an old building then demolish it to construct a tower.
- If land is available to build a tower it will be very expensive.
- Building code regulations in urban areas are very strict and it will be very difficult to obtain building permits for an antenna tower.
- Urban areas require expensive surveys prepared by engineers to submit to the municipality as part of the building plan submissions.
- If the tower does meet building code then residents located near to the proposed tower project will complain when the municipality holds a hearing to discuss the construction.
- If an urban tower is built then the annual property taxes will be high.

Mobile phone companies have to install antennas in urban areas to provide coverage for customers. Their first option is to locate a tall building to install the antennas, and their second option is to work with a tower erection company who has gone through the lengthy process of constructing a tower for mobile operators. The mobile phone company will only look at constructing a tower when all other possibilities have been exhausted. Even when specialist companies are able to construct towers in urban areas there are many restrictions placed on the construction, such as a limit on the height of the tower, which is a limiting factor for the range of transmission.

4.6. Point to multi-point when Internet is available at the location

It is likely that a tall building in an urban area can have an Internet circuit of some type installed. A mobile phone antenna tower will have Internet access available because it is required by the mobile phone carriers. Before entering into an agreement with the Internet service provider ensure that the service can be resold. This will require contracting a more expensive business account for the service; do not contract a residential account. When the PtMP antenna is connected to an ISP service at the PtMP site then the WISP has to choose one of two options to control the customer's access to the Internet and the rate plan that is applied for each customer.

- Configure a VPN (Virtual Private Network, sometimes called a 'tunnel') at the tower location to connect the customer back to the NOC for access control.
- Install a remotely managed access control router at the PtMP location.

The VPN solution will permit the WISP to manage all access control tasks through one router at the NOC. However there are disadvantages:

- The WISP has the additional expense of a VPN router at the tower site and also at the NOC site.

- The NOC inbound data traffic will travel over the wholesale data circuit, not the wireless distribution network, and so the wholesale circuit capacity will have to be increased.

The VPN will therefore add costs that do not occur with a PtP wireless backhaul from the site to the NOC. A figure illustrating the VPN connection is shown below.

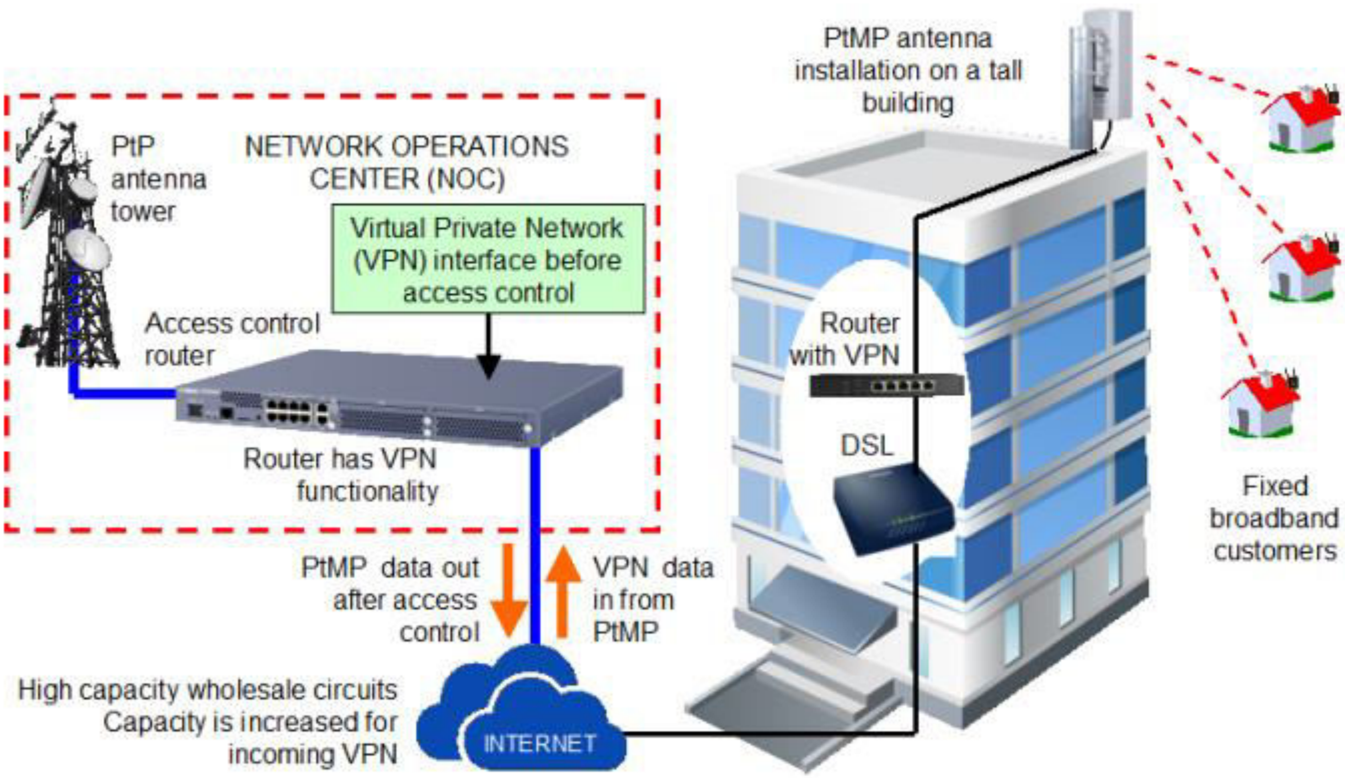


Figure 4.6.1. PtMP to NOC configured with a VPN link via the ISP circuit.

Installing an access control router at the PtMP tower site is the lowest cost option, the data does not have to be routed via the site ISP connection through the NOC and the cost of the PtP wireless backhaul to the NOC is eliminated. The WISP has to configure the access control router remotely, which is not a great burden if the control is manual or automated. The WISP then will have two or more routers to configure. If the WISP chooses a management and billing software that has an interface to the access control routers then the configuration of the router is transparent to the WISP. The next diagram shows the installation of the PtMP tower site with the access control router remotely managed via the Internet.

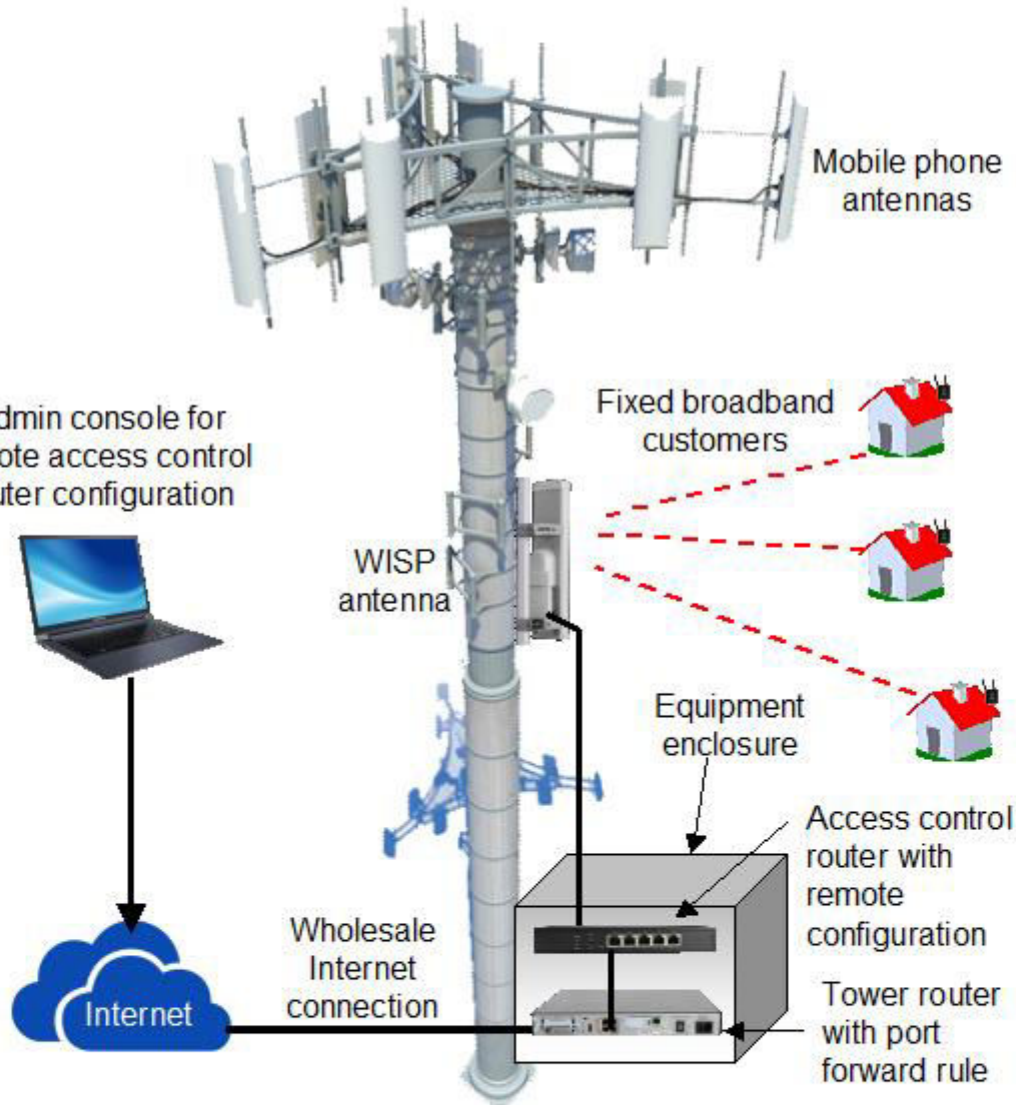


Figure 4.6.2. PtMP with access control at the tower site and connected via the ISP circuit.

4.7. Networks in dense urban areas where LoS is limited

When connecting residential and business buildings to a PtMP antenna in a dense urban area it is likely that tall buildings will block the line-of-sight (LoS) signal path between the PtMP and some CPE antennas. There are two solutions for this problem.

- Install relay/repeaters at points in the urban area to provide coverage in the RF shadow of large buildings.
- Install mesh wireless CPE units, which will function as repeaters to other CPE mesh units.

The relay/repeater will be installed at a high point, probably the roof of a tall building, so the installation will have the same issues as those issues when installing the PtMP antenna; there will be the cost of the location rental and permits will be required to approve the installation. In some cases it might be possible to negotiate with a customer for permission to put a repeater at the customer's site if that site will give LoS to other prospective customers who have no LoS to the PtMP antenna. The figure below illustrates the installation of the relay/repeater to provide an RF signal for customers who are behind the tall building and therefore have no LoS to the PtMP antenna.

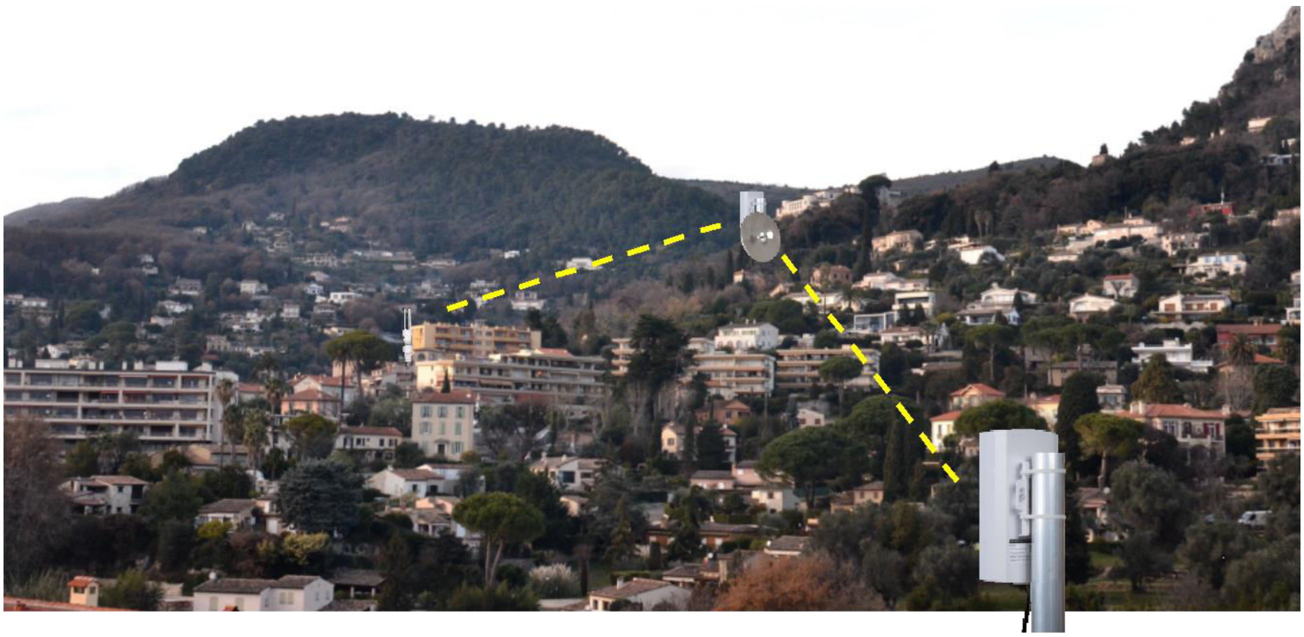


Figure 4.7.1. A relay/repeater installed to give RF coverage in the RF shadow of a tall building.

A wireless mesh is built with wireless units that are both CPE and wireless access points and have routing functionality. The wireless access point rebroadcasts the RF signal received by the CPE wireless. The mesh wireless can use a single radio that is alternately switched between CPE and AP modes, however better performance is obtained using two radios, one that is configured as a CPE and the second that is configured as an AP. Each customer installation is made with a mesh wireless instead of a CPE wireless so that it can connect other customers to the network. The mesh wireless product has routing functionality to determine the path from the Internet to the antenna that connects the customer. The connection might require several 'hops' through the mesh network. The routing software maintains a table of each device in the mesh so that the transmission from the customer CPE to the PtMP antenna can travel by the shortest route, with the fewest number of 'hops'. The routing software therefore is selective when re-transmitting a data packet received by the CPE so that the packet is only retransmitted when it is in the shortest route path. Technically mesh is an excellent solution to connect many customers to a PtMP antenna however it has a drawback, the performance or speed of transmission drops with each additional 'hop' through the mesh network, therefore the customer cannot have a guaranteed maximum data speed. This situation might be acceptable for a community wireless network where users share resources and have no agreement for the quality of service, however a WISP is selling rate plans and must honor the network performance that has been promised to the customer. The figure below shows how mesh wireless units might form a wireless network within a city that has buildings, which may block the LoS to the PtMP antenna.

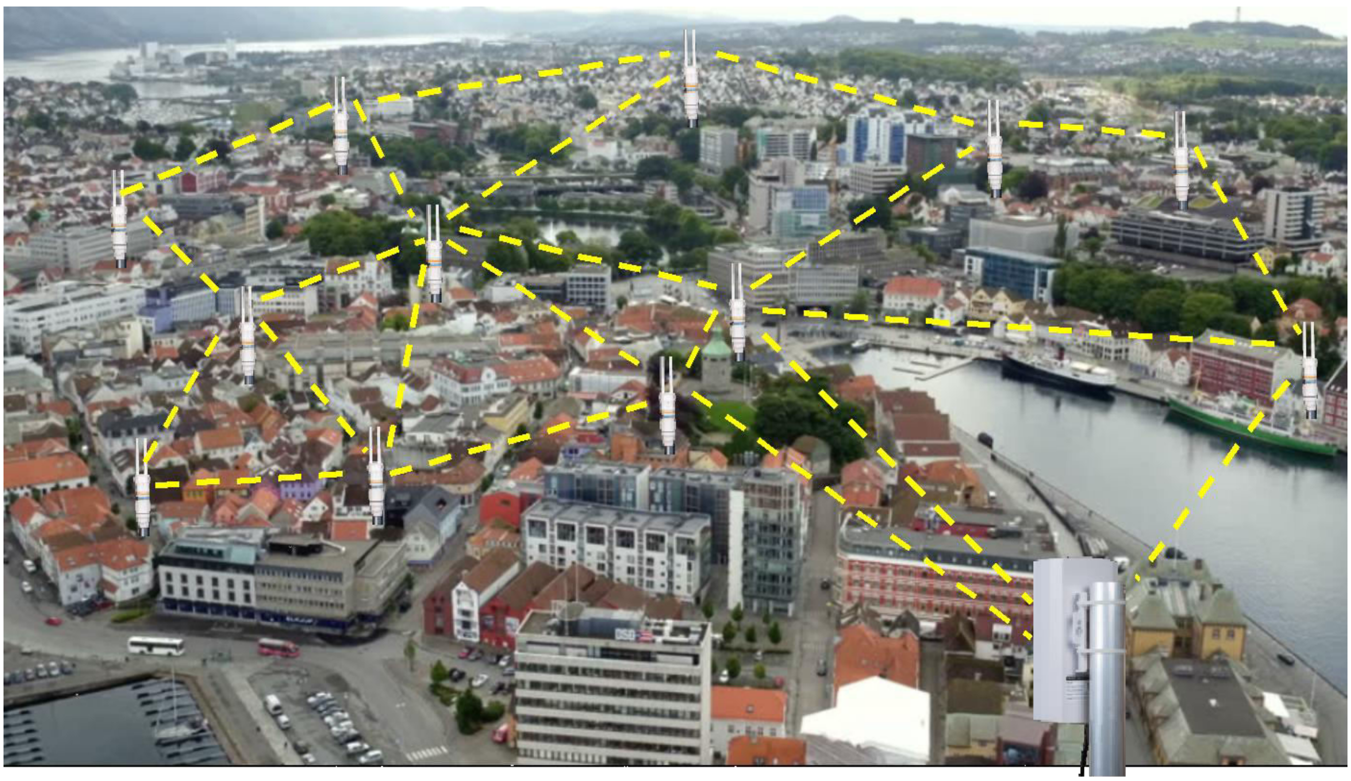


Figure 4.7.2. Wireless mesh CPE/AP units which forward data packets to locations that have no LoS to the PtMP antenna.

4.8. Urban multi-residential and multi-office buildings

One special case that the WISP will encounter when installing a wireless network in an urban area is the multi-residential dwelling building and also the multi-office building. It is not possible to provide each tenant with a CPE wireless on the roof of the building so the solution is to install one CPE wireless on the roof of the building and then wire Ethernet cables inside the building to every tenant. Each tenant is provided with a wireless router and the authentication credential is programmed into the router, which is locked down with a password. Each tenant wireless router is therefore authenticated independently at the NOC and the correct rate plan is applied to each tenant. The figure below shows the connection of a multi-tenant building to the NOC via a PtP wireless connection.

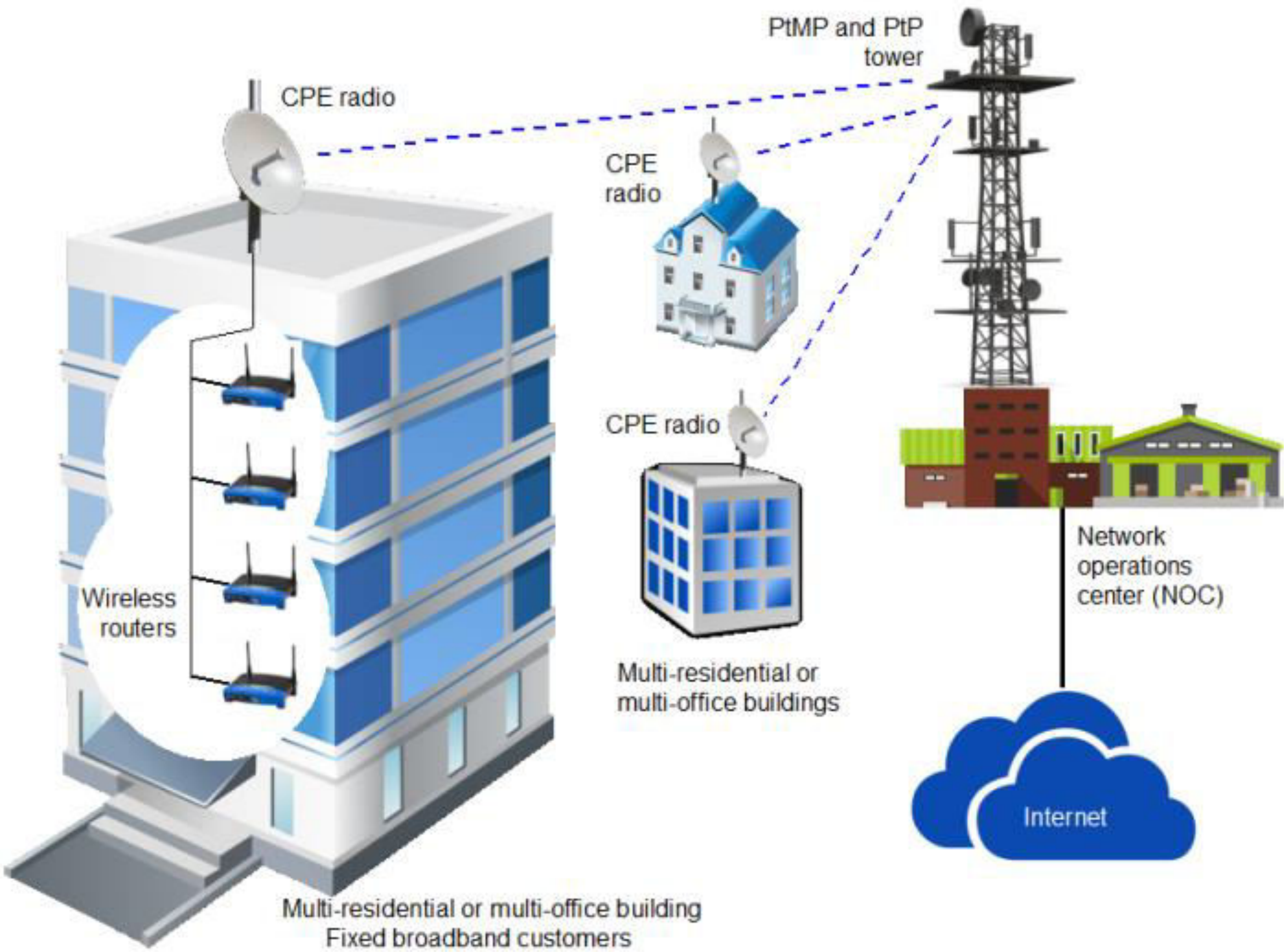


Figure 4.8.1. Providing Internet service for multi-residential and multi-office buildings with a backhaul to the NOC.

If the building can be provided with a high bandwidth Internet circuit such as fiber then the WISP can connect the tenant wireless routers to an access control router installed in the building and manage the access control functions of the tenants remotely. The access controller at the NOC will require periodic management of the building customers. When access controllers are installed at each multi-residential or multi-office site they will require remote management via the Internet. If the access control router is behind a router installed by the ISP then the ISP's router will require a port forward rule installing to permit remote access to the access control router. If the ISP can install a modem then the access control router WAN port can be configured with a public IP address facilitating remote access. The next diagram illustrates the installation of an Internet service for tenants of a multi-residential or multi-office building with the Internet service provided by a wholesale ISP.

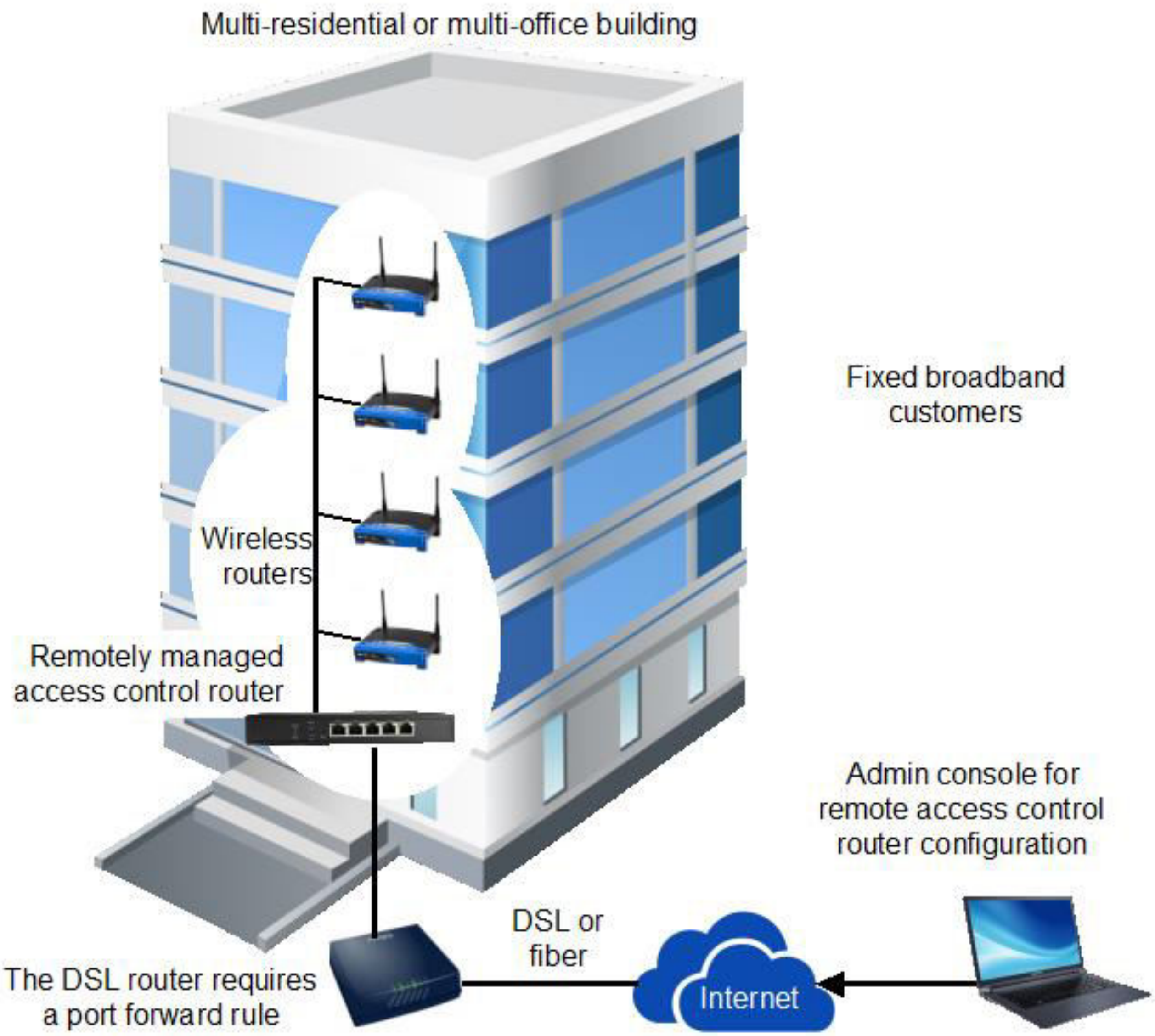


Figure 4.8.2. Providing Internet service for multi-residential and multi-office buildings with an Internet connection to an ISP.

There is an alternative Internet solution for a multi-tenant building where a mobile broadband service is provided instead of a fixed broadband service. This is similar to the service provided for a hotel. The WISP will install wireless access points along the corridors on each floor of the building. The tenants can connect mobile devices wirelessly to the wireless access points using an access code that is purchased from the WISP through the sale of a voucher, or else purchased on-line. With this on-demand Internet service the customer will purchase Internet access for a fixed period of time, rather than pay monthly as a subscriber. The WISP will prefer to have monthly subscribers to guarantee cash flow, however the on-demand solution will simplify the building network installation and reduce the initial cost of generating revenue from the building tenants. In the case where the WISP installs a wireless router in each apartment or office of the building the wiring work will be much greater than installing wireless access points in the building corridors.

The WISP will find situations where the owner of a multi-tenant building wishes to provide an Internet service for the tenants and then add the cost of the Internet service to the monthly rent. The WISP will install the network infrastructure inside the building and then charge the building owner a monthly fee for the service.

4.9. Point to multi-point installations in rural areas

In a rural area the WISP might find a tall structure such as a farmer's grain silo or a municipal water tower to install a PtMP antenna but such structures are rare not common and not in the best location for a PtMP antenna. When building a PtMP antenna in a rural area the first approach is to look for an area of high ground to install a PtMP antenna in order to have the maximum possible range so that as many customers as possible are included in the coverage area. If the hill that is found to install the PtMP antenna is a high point in relation to the surrounding area then it is possible that no tower construction is required. The NOC will be constructed at a location where there is electrical power and where the wholesale broadband provider can deliver a data circuit. The NOC location will have a PtP wireless link to the tower so there must be LoS between the NOC and the tower. If no LoS then an intermediate relay/repeater will be installed at some point between the NOC and the PtMP tower to provide the wireless PtP connection. If the land is flat then a tower will have to be constructed at a point that will give coverage to a large number of potential customers. The tower PtMP and PtP equipment will be powered by a solar panel and wind turbine with battery storage. The WISP will also have to negotiate with the landowner to pay rent for the location however the cost will be much less than for a tower located in an urban area.

The density of rural customers will be low and so the WISP should carefully analyze the prospective customer area to ensure that there will be enough customers to achieve break even with the tower installation. Too few customers will mean that the tower installation will never make a profit, as the cost of delivering the Internet service will exceed the revenue from customers.

The diagram below illustrates a rural PtMP antenna installation.

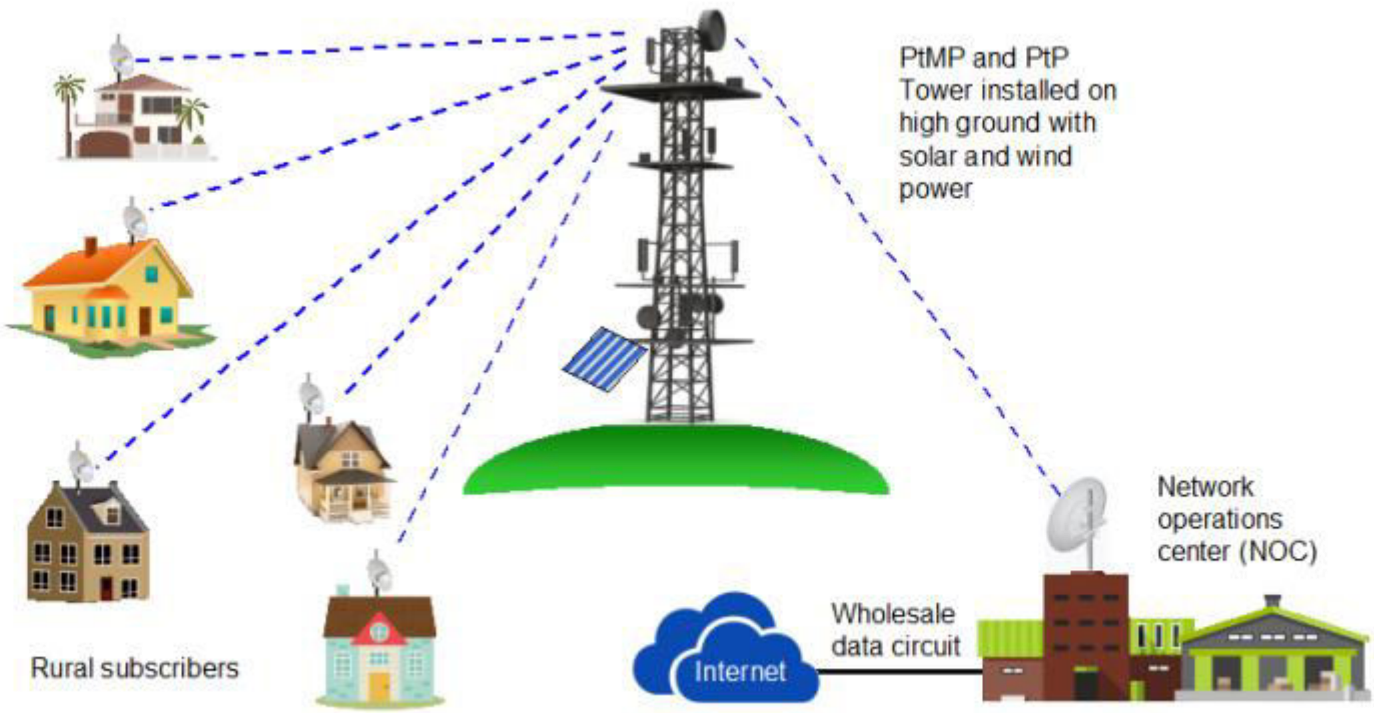


Figure 4.9.1. A Rural PtMP antenna installation.

4.10. Using a satellite connection as a NOC trunk circuit

There are many locations in the world where a WISP would like to provide an Internet service but it is not possible to have an ISP Internet connection due the remote location, where the nearest ISP point of presence might be hundreds of Km distant making it impractical to have a multi-hop wireless link to the WISP's location. There are determined WISPs who will use a geo-stationary satellite link as a backhaul for the NOC however the few services available are expensive and intended for one customer only. The download and upload speeds are a few Mb/s whereas the WISP needs a backhaul speed in the range of a few hundred Mb/s. In addition the satellite service providers will charge for the data that is transferred at a cost per Gbyte. There are many WISPs using the Hughes satellite service because it is the only method to offer Internet service, however the quality of service provided to customers is the basic minimum. For potential customers who have no other alternative to get Internet the solution is acceptable. Twenty-five years ago a 56Kbit dial-up modem to AOL was the standard of Internet access. The following diagram illustrates the NOC backhaul connection via a geo-stationary satellite.

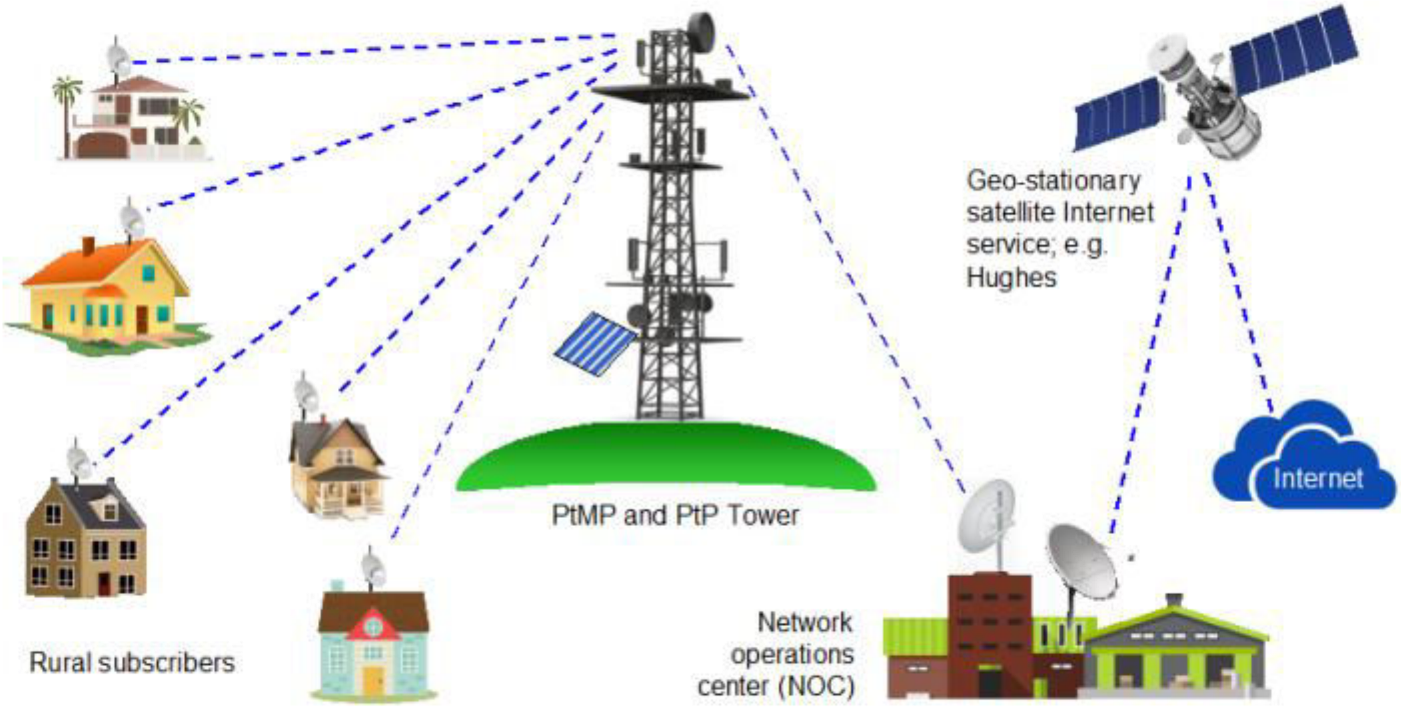


Figure 4.10.1. NOC backhaul to the Internet via a geo-stationary satellite.

Low Earth Orbit (LEO) satellites that are presently being launched to compete with geo-stationary satellite technology. The LEO satellites will provide higher data rates with lower latency than geo-stationary satellites, with a cost slightly higher than geo-stationary satellites. Geo-stationary satellites have directional antennas that provide a connection on specific areas of the earth, while LEO satellites will provide total earth coverage, excluding the poles. A LEO enterprise service for businesses that sell Internet services will have a higher cost than the service for residential customers. LEO satellites will be a great benefit for WISPs around the world because it will be possible to use satellites as the Internet backhaul and provide a good quality service for customers. A WISP can provide a lower cost service to customers who cannot afford the LEO satellite receiver by sharing one LEO antenna between several customers, each with a lower data rate. There is a cost reduction benefit for the WISP because a LEO satellite antenna can be installed at the PtMP tower site, which will eliminate the wireless distribution network between the PtMP tower and the NOC, and eliminate the NOC. LEO satellite technology promises to revolutionize the WISP industry when an enterprise service is available.

4.11. Distributed network design using cloud management

Distributed network design means that some network functions that were centralized in the NOC are distributed throughout the network. There is a good reason to do this; the NOC is a single point of failure, if one component of the NOC malfunctions then all customers loose Internet access. A large investment has to be made to build redundant systems in the NOC, such as backup power supplies. Distribution of functions means that a failure in any one component may mean that only some of the subscribers are without Internet; still not a good situation but better than having all customers without Internet. Examples of function distribution are listed below.

- When subscriber management and network monitoring software is hosted in the NOC the WISP has to install backup power supplies in case of a power outage and real-time backup to a second server with hot swap in case of a server failure. Software used by the WISP for subscriber management and network monitoring can be hosted on a cloud service like AWS, which has backup power and real-time data backup. This will eliminate one of the points of failure.
- The access control router is critical to the operation of the WISP and a failure of this device at the NOC will prevent customers getting access to the Internet. The WISP will need backup power for the router and a second router on standby. As an alternative the WISP can install a smaller access control router at each tower site and in the case of a router failure only the customers who are serviced by that tower are affected. The tower will have backup power for the wireless equipment and the router. Equipment failure is still a problem but fewer customers will be affected so the risk to revenue loss is reduced.
- If the WISP has more than one wholesale broadband provider who can supply Internet service then each tower can be connected to the closest provider, which will reduce the complexity of the wireless distribution network.
- When the WISP has access to a LEO Internet service provider then a LEO ground antenna can be installed at each tower eliminating the wireless distribution network.

It is clear that when the NOC functions are distributed throughout the network then the NOC can be eliminated, improving reliability by eliminating a single point of failure, and eliminating a major operating expense. The WISP might need only a business office with warehouse for employees to work and to store equipment ready for network installations. All management software that the WISP requires to run the business is either hosted by the WISP on a cloud platform, or else the WISP contracts with a cloud service provider.

The availability of LEO satellite backhaul connections will permit entrepreneurs to begin offering Internet services in parts of the world that are currently not possible to service. Only a small part of the globe has Internet access concentrated in urban areas. Many rural areas do not have Internet services. As LEO Internet services become available then LEO antennas can be installed on each PtMP tower. Distributed management of the network is essential when each PtMP tower has a backhaul to the Internet via a LEO satellite.

Each tower access control router can be configured manually. The WISP may also contract with a cloud WISP management system vendor who provides an interface to a router such as that manufactured by Mikrotik making it a plug-and-play system. In this case the WISP entrepreneur need not be concerned about learning how to configure and program routers.

The figure shown below illustrates to configuration of the PtMP tower for distributed operation. The only change from the tower that WISP's are currently using is the addition of the access control router between the PtMP antenna and the backhaul PtP antenna. The access control router only implements access control for the customers who are connected to that tower. Some vendors might include the access control software in the PtMP access point.

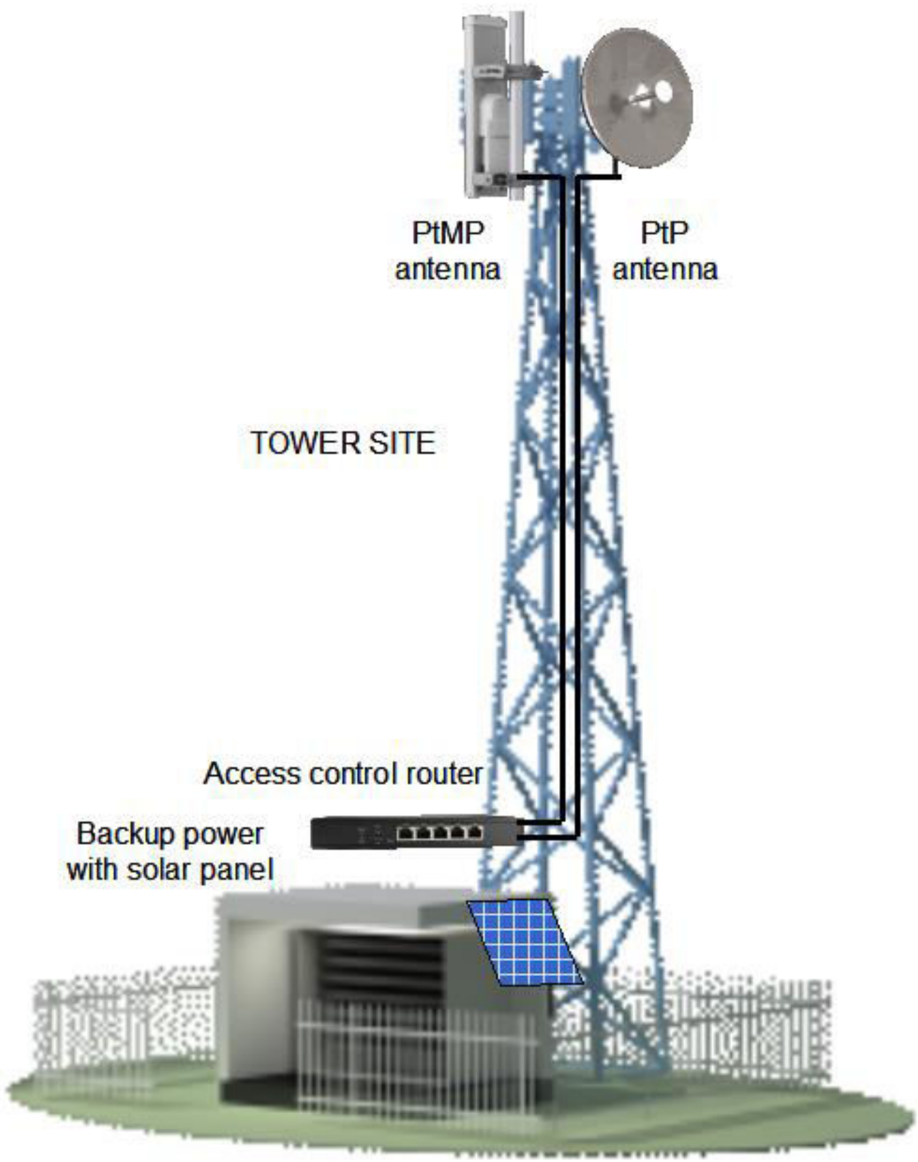


Figure 4.11.1. WISP PtMP tower configured for a distributed network.

The next figure shows what a distributed network might look like. Each tower can connect to the most convenient Internet service where access to the service is the shortest distance to the tower. Different towers may connect to different service providers, including geo-stationary or LEO satellite service providers. Some cloud management systems can administrate such a network in a very transparent manner so that the WISP sees only one network via the management portal, not several different networks.

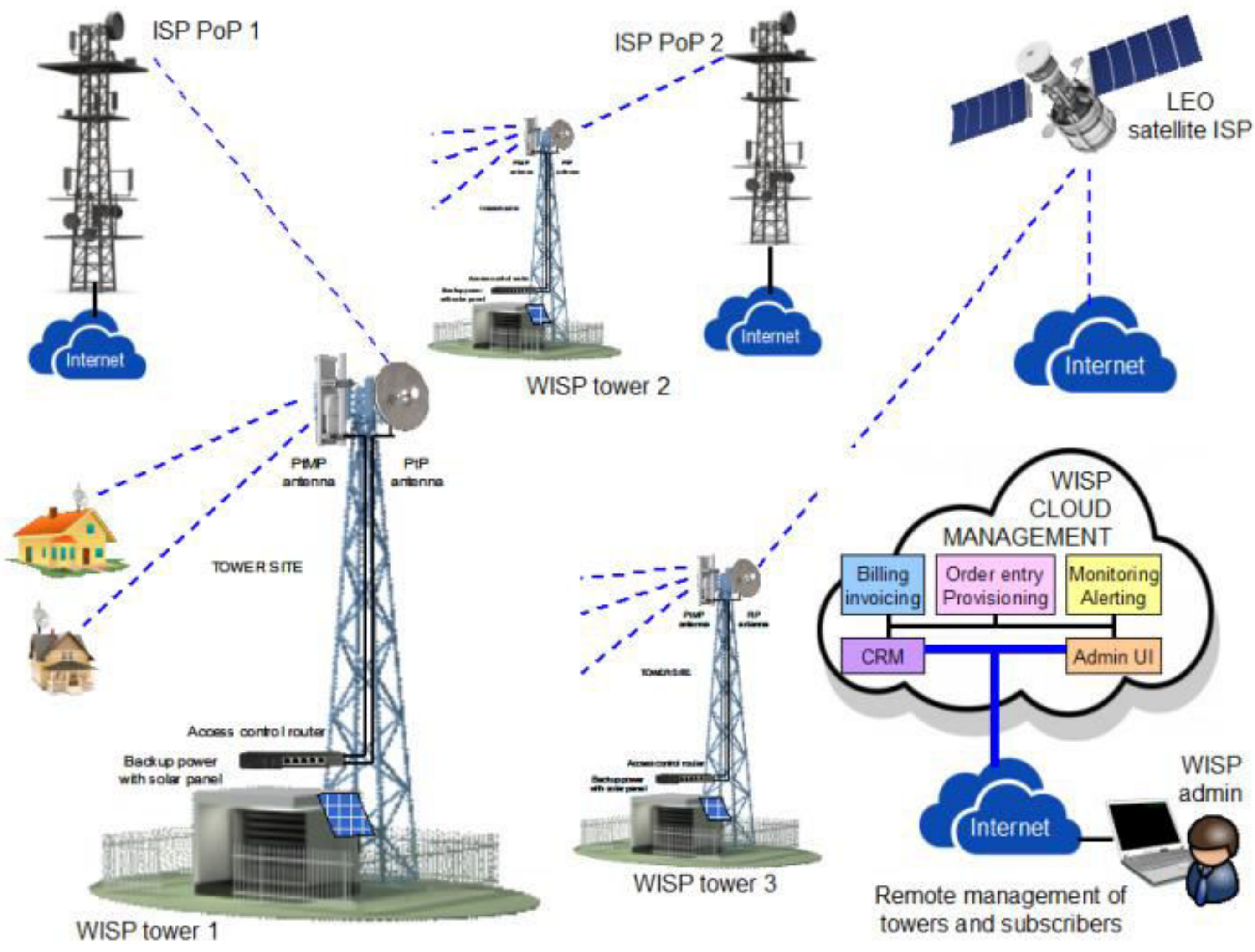


Figure 4.11.2. WISP network with distributed components and management.

4.12. Distributed network design access control solutions

The WISP is accustomed to using a router for the subscriber access control functions. The previous section illustrated how a small router can be installed at each tower for distributed access control of subscribers accessing that tower. Some PtMP wireless access points and some CPE wireless units are also programmable routers. Examples of this are the Routerboard range of products that are manufactured by Mikrotik. The access control scripts can be added to a PtMP wireless access point or to a CPE wireless unit. If these devices were to be programmed manually then the workload that the WISP has would increase, however some of the cloud management systems can manage multiple units, either PtMP wireless access points or CPE wireless units.

Figure 4.12.1. The Mikrotik SXT SA5 14dBi integrated Sector AP, 90 degrees beam-width, Gigabit Ethernet, with RouterOS that can have scripts added to function as an access controller when deployed together with a cloud-based WISP management system.

Figure 4.12.1. The Mikrotik SEXTANT is a 18dBi 5GHz 18dBi integrated CPE/Backbone antenna with Gigabit Ethernet. The RouterOS software permits adding scripts to function as an access controller when deployed together with some cloud-based WISP management systems.

4.13. Adding redundancy to the network design

When planning a network design, redundant design features are introduced to improve the reliability of those parts of the network that are considered to have a higher probability of failure. Redundancy of NOC systems includes the backup power generator that will power the NOC in the event of a power failure of the utility. It is possible to draw up a list of the weakest parts in the network and plan how to build redundancy to improve network resilience.

Electrical power supplies in the power grid of any country in the world are always interrupted by some weather condition. The WISP has to assume that power outages will occur and plan accordingly. The NOC requires a large amount of power and so will require a gasoline generator to provide power when a power utility failure occurs. A gasoline generator does not start instantly and so the backup power supply will also include batteries to provide power through an inverter until the gasoline generator reaches the correct output. Voltage monitoring electronics monitor the line voltage, battery inverter voltage and generator voltage to change the 3-way switch accordingly so that the NOC never looses power. Power backup for the NOC is illustrated in the next diagram.

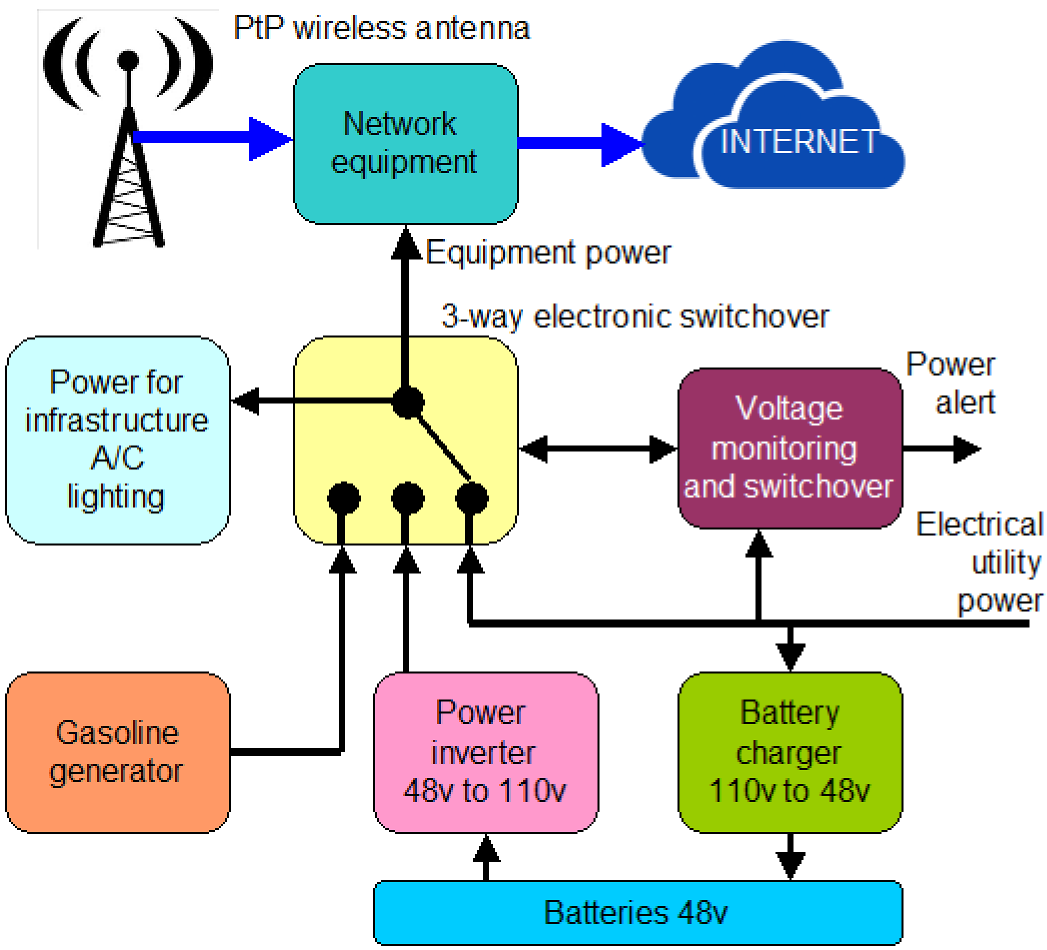


Figure 4.13.1. Network operations center redundant power backup.

Each PtP and PtMP tower installation and PtP relay/repeater installation that is powered by the electrical utility will require a battery backup supply to power the equipment when a power loss occurs. Fortunately the PtP and PtMP wireless installations consume very little power, usually less then 10 Watts and so a backup battery can power the installation for several days. Environmental monitoring should be included at each site so that the WISP is alerted when a power loss occurs. No power switchover is required, the equipment is always powered from the battery, and the battery is constantly charged by the utility power. If the utility power fails then the equipment continues to be powered from the battery. When the utility power fails the monitoring equipment will send a message to the administrator. The monitor also measures temperature and humidity and sends this information to the administrator.

The diagram below shows the components that are required to power the PtMP tower and the PtP relay/repeater towers when connected to utility power. If the WISP installs the PtMP antenna at an antenna tower that is used by mobile phone carriers then the tower owner will provide the power backup and conditioning.

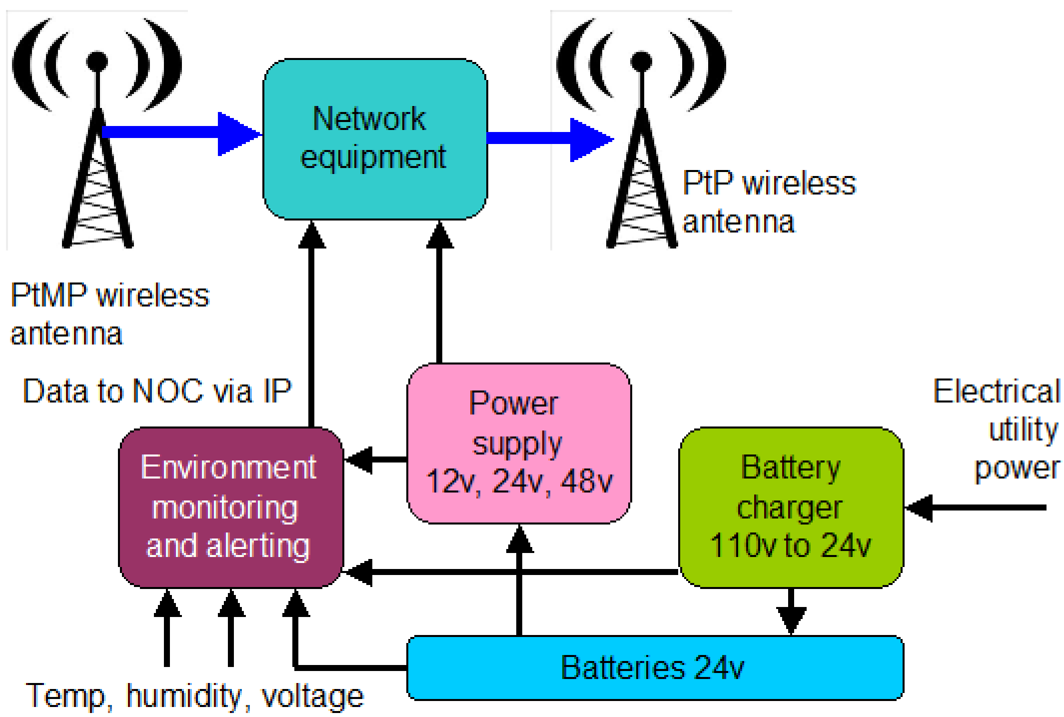


Figure 4.13.2. PtP and PtMP wireless site backup power system powered by the utility.

When the tower site does not have utility power the battery charger is replaced with a power supply that takes power from a solar panel and wind turbine to charge the battery. The next diagram shows the power backup system when the tower is powered by wind and solar energy.

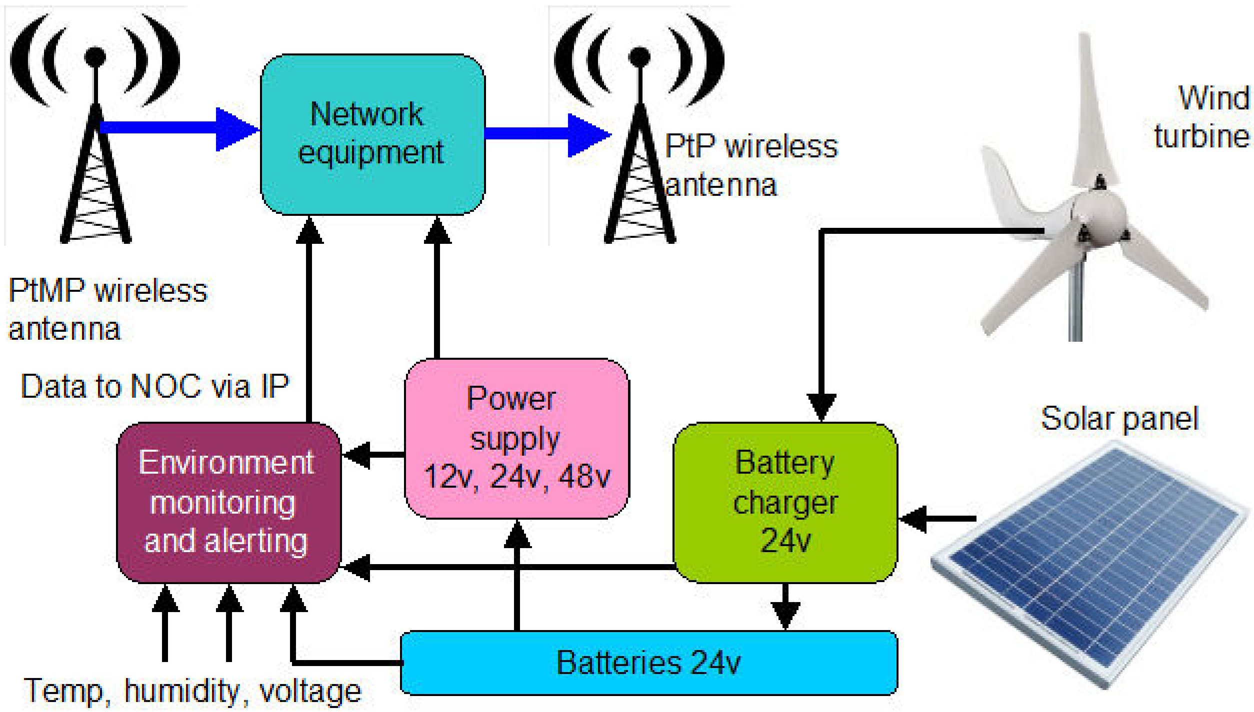


Figure 4.13.3. PtP and PtMP wireless site backup power system powered by solar and wind.

ISP circuits that connect the NOC to the Internet are prone to outages that are outside the control of the ISP. The ISP will connect to a circuit using copper or fiber cables, which either pass overhead on poles or else buried underground. The NOC might also connect to the ISP's point of presence (PoP) through a high bandwidth wireless point-to point-link. When possible the WISP should contract two wholesale circuits from two different ISP's for redundancy of the NOC Internet connection. This must be two different ISP's because two circuits from the same ISP will connect via the same cable so there is no redundancy benefit. Contracting two circuits will increase the operating cost but will lower the probability of outages for the customers. The NOC connects to the two circuits via a load balancing router that has automatic fail-over. In normal operation the WISP can combine the throughput of the two circuits to provide a higher bandwidth circuit and consequently support more customers. In the case that one of the ISP circuits fails the router will switch data traffic over to the ISP circuit that continues to function. This will reduce the backhaul throughput to the Internet and the result will be that customers experience slow Internet speeds, however customers will not loose Internet access.

The following figure illustrates the NOC installation with the router configured for dual-WAN to provide load balance and fail-over. It does not matter that the two ISP circuits might be different types or different speeds, for example one circuit is fiber and a second circuit is wireless. The WISP can connect additional circuits as the router can be configured for any number of WAN ports, only limited by the number of Ethernet ports on the router.

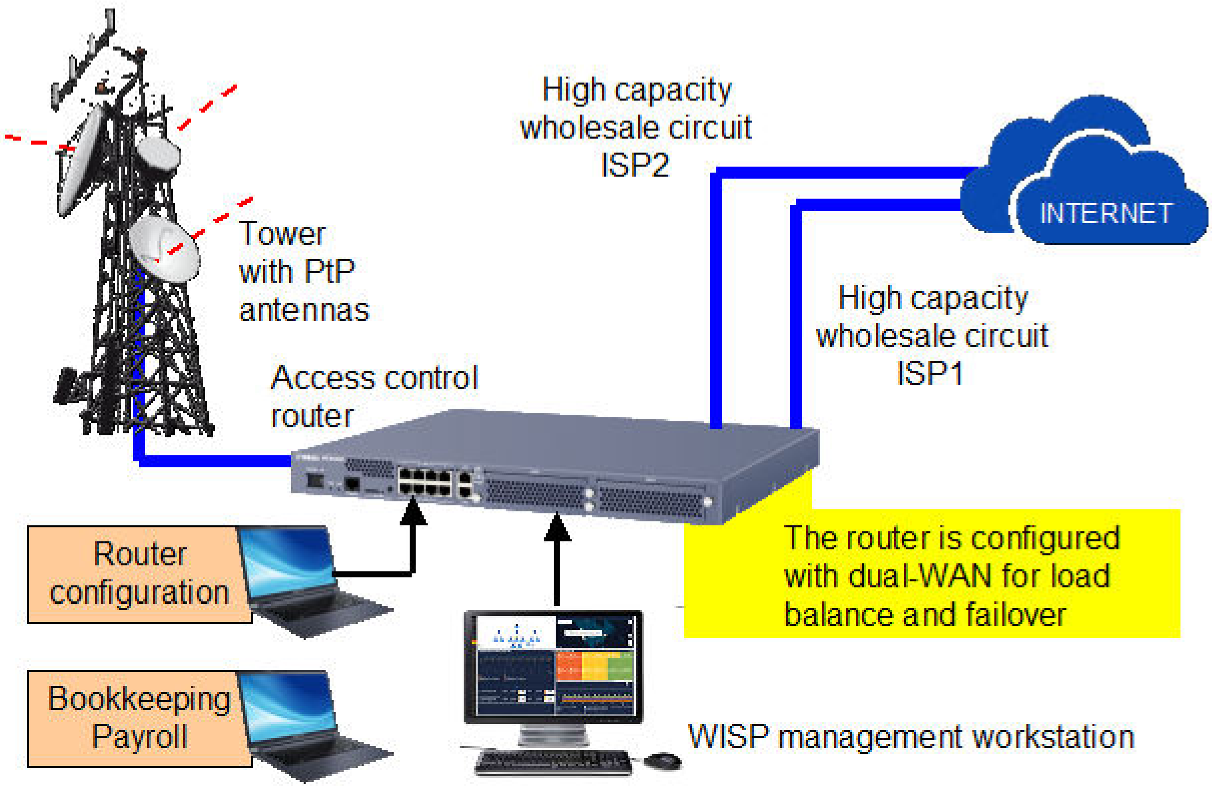


Figure 4.13.4. NOC load balance and failover for two ISP circuits.

The point-to-point data links are a weak point in the WISP network, especially multi-hop links that are part of the wireless distribution network. The problems with PtP links occur for a number of reasons.

- Deterioration of outdoors equipment caused by the weather.
- Change in vegetation along the path of the PtP link, trees grow and eventually appear in the Freznel zone of the transmission path reducing the signal to noise ration of the connection hence reducing the data rate.
- The damaging effects of animals that chew cables and climb onto equipment, a tall tower with a few antennas on top is a great place for a large bird to build a nest.

The WISP must make periodic inspections of every part of the wireless distribution network to ensure that the equipment remains in good operating condition, and replace equipment that is deteriorating. In critical parts of the wireless distribution network the WISP can duplicate links over different paths for redundancy. Redundancy is implemented by installing a load balance/fail-over router at the PtMP tower that connects to two backhaul PtP antennas, each one connecting to the NOC over a different path.

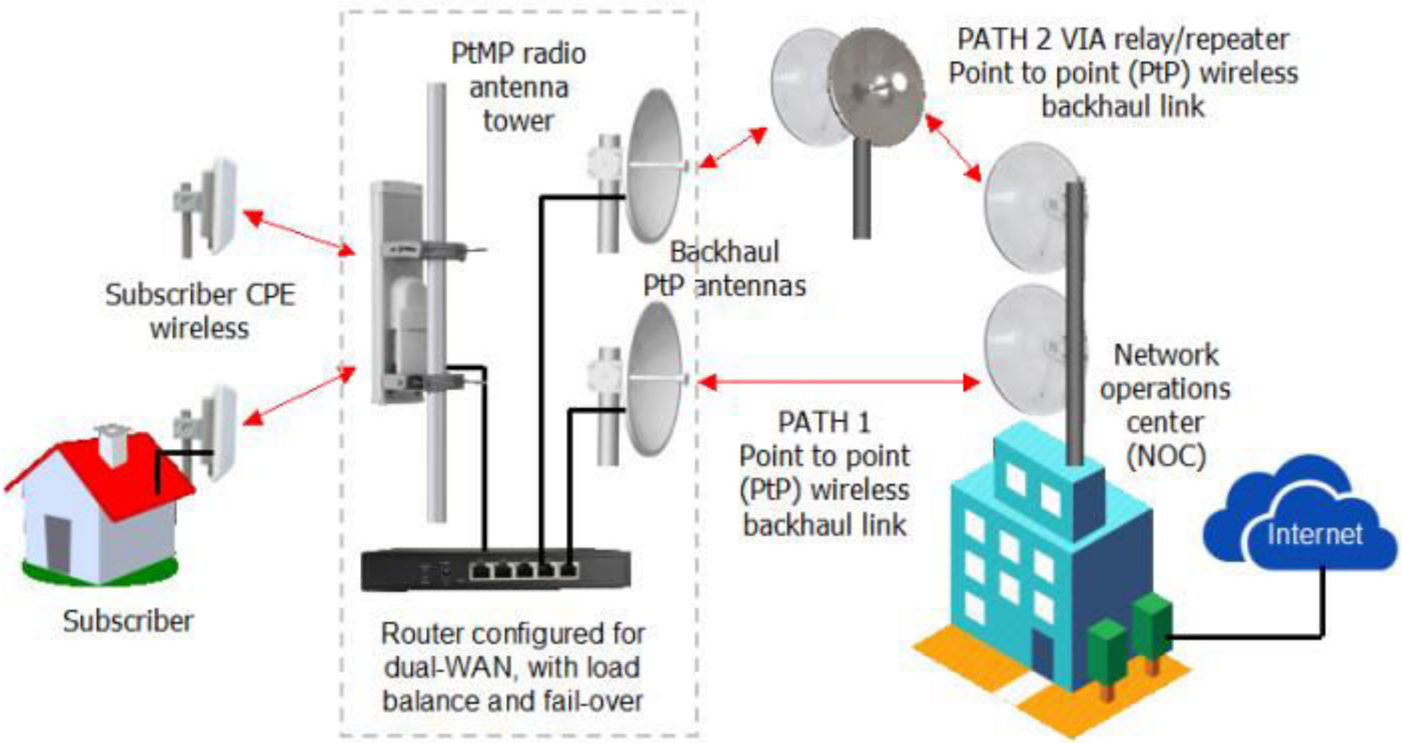


Figure 4.13.5. The PtMP tower with two backhaul PtP paths for redundancy.

4.14. Centralized vs. distributed network design, pros and cons

Almost all WISP networks are built with the centralized model for the reason that a wholesale ISP provides a high capacity data connection at one location and the WISP has to build out the network from that point. The WISP's area of coverage is restricted to areas where wholesale ISP’s can provide backhaul connections. In some parts of the world there are no wholesale ISP's and WISP's are backhauling their PtMP towers into DSL circuits when available or geo-stationary satellite circuits such as those provided by Hughes in areas of the world where this service is available. Consequently the quality of service provided to customers is extremely variable, however customers who want Internet access in some parts of the world have no other alternative than to use poor quality services. Many large areas of the earth have no Internet service, as there is no access to an Internet backbone connection.

WISP's will soon have the opportunity to provide Internet services in areas where it is not possible today. The introduction of LEO satellite Internet services will permit tower backhaul connections at any point on the earth, and not limited to the locations with a copper or fiber cable. People in many parts of the world cannot afford the cost of LEO satellite services but the performance of the service is sufficient to provide a WISP tower backhaul into the Internet. The WISP can divide the LEO satellite cost between many people so that the service becomes affordable for each customer. A new generation of WISP's will start in business to provide Internet for locations where the Internet service is currently not possible due to the lack of any type of backhaul connection to the Internet backbone.

Regarding the network transition to LEO satellite backhauls, it was noted previously that LEO satellite antennas could be installed on each PtMP tower. Each LEO antenna will provide the backhaul bandwidth for a group of customers. Multiple LEO satellite antennas cannot be installed at the NOC because several LEO antennas grouped together would share the bandwidth from one satellite, which gives no throughput advantage. However when LEO antennas are installed on towers spaced by several Km each LEO antenna will communicate with a different satellite.

When LEO satellite services finally become widely available in an enterprise service form that permits WISP’s to resell the service then existing WISP’s can switch to distributed network designs and new WISP’s will start with distributed designs.

A WISP can begin the process now of upgrading the network to be ready for LEO antennas. The change requires moving the large access control router out of the NOC and installing smaller access control routers at each tower for those customers that are accessing that tower. For the WISP who is configuring the central access control router manually then having access control routers at each tower will represent an additional workload. There are cloud WISP management systems that can interface with multiple access control routers and so the WISP might consider migrating the business management to such a cloud system. The WISP who is adept at programming and may have built an interface between the management software systems and the access control router can upgrade the management system to work with multiple routers where one is installed at each tower.

A WISP who already has a wireless distribution network and NOC can keep that network infrastructure and add a LEO antenna at each tower to increase backhaul throughput and then add more customers to the PtMP antennas installed on the tower. The WISP will require the addition of a router configured for access control and for dual-WAN with load balance and fail-over.

A table is included to illustrate the differences between centralized and distributed network implementations.

Characteristic	Centralized design	Distributed design
Single point of failure.	The NOC is a single point of failure, any failure will stop Internet access for all customers.	Each tower is a point of failure, any failure will stop Internet access for the customers of that tower, other customers will not be affected.
Tower power redundancy.	Backup battery with utility power or else solar/wind power with battery.	Backup battery with utility power or else solar/wind power with battery.
Tower data redundancy.	Add dual PtP backhaul connections from the tower to the NOC for redundancy.	Add dual PtP backhaul connections from the tower to the ISP PoP for redundancy.
NOC power redundancy.	Backup generator with battery storage for switch over on utility failure.	No NOC.
NOC data redundancy.	Add redundancy through two or more high bandwidth backhauls to different ISPs.	No NOC.
Automated management of access control.	Management software installed at the central NOC site, however the WISP can host with a service such as AWS.	Cloud based management, either the WISPs own software hosted in a cloud service, or else the WISP can use a cloud service provider.
Systems redundancy.	NOC systems that automate the interface to the access control router may stop authenticating customers if the systems fail.	Cloud management systems that automate the interface with the access control router will continue operating when contact with the cloud is interrupted.
Ease of use.	The WISP network is managed from the NOC, however remote access to the NOC can be configured for management.	All management and administration is cloud based so the WISP can manage from anywhere with an Internet connection.
Upgrade ISP backhaul to tower based LEO satellites.	The centralized network will require changes in design to accommodate LEO tower backhaul antennas.	The distributed network is ready for the LEO backhaul antenna installation at each tower.

Table 4.14.1. Comparing the characteristics of centralized network design with distributed design.

4.15. Special requirements for business customers

The WISP customer portfolio will include businesses that seek more services than the residential customer requires. Businesses might request the WISP to provide IT services that are related to networking. A small selection of services that a business customer might ask the WISP to provide are listed below.

- Installation of network infrastructure inside the business building.
- User tech support for business employees.
- PC installation and configuration.
- Cloud installation of 3rd party applications, e.g. Microsoft Azure, Amazon AWS.
- Off-site data backup storage.
- Disaster recovery; crashed disks, viruses, Ransomware attack.
- 24/7 monitoring, with 4-hour repairs.
- Internet Hotspot service for guest and visitors.
- Virtual PBX IP phone system.
- Security systems that include IP cameras with hosted DVR.

The WISP might be able to establish partnerships with IT service firms who operate in the WISP's coverage area so that a broad range of services can be offered to business customers. Most of the items on the list are services that IT firms provide. There are some services however where the WISP can take advantage of the network infrastructure to provide the service.

The WISP NOC can have additional servers installed for services that include off-site data backup storage and hosted DVR for security systems. The WISP can contract with an IP phone provider to resell the IP phones service to business customers. Residential customers may also be interested in this service. The WISP has infrastructure to monitor network components, this can be extended to monitor products at customer sites and issue alerts for customers.

Some types of business customers need an Internet Hotspot service for their guests and visitors. One type of business segment that needs this service is hospitality, which includes motels and hotels. This mobile broadband service requires the WISP to install Hotspot infrastructure at the customer's site. The customer may want to control guest access to the Hotspot and so the installation will require a mechanism to generate access codes or vouchers with the code printed. There are several types of Hotspot controllers that the WISP can install at the customer site, which will provide the guest Internet service.

4.16. Summary

The key points or take-a-way's that a WISP entrepreneur should remember when planning the network design are listed below.

- Look at the business proposal for the planned area of coverage and plan how the centralized network will be designed to service the target customers.
- Plan the NOC installation at a location where the ISP can deliver the wholesale connection and PtP links can be installed to each tower. Prepare a budget for the installation, products and backup systems that are required.
- Plan integration of management systems within the NOC for customer authentication, automation of activation and rate plan settings, and alerting of failure monitoring.
- Prepare a plan for locating the PtMP antenna to give maximum coverage for prospective customers.
- Check the criteria for installing a PtMP antenna in an urban area.
- Check if an Internet circuit is available at the chosen PtMP tower or building location.
- Consider the technical solutions for dense building areas where LoS is limited.
- Plan to provide an Internet service in a multi-residential or multi-office building.
- Considerations when locating a PtMP antenna tower in a rural area.
- Plan the use of a satellite connection as a PtMP tower backhaul.
- Consider a cloud WISP management system to build a distributed network design.
- Access control solutions for a distributed network design.
- Improve network reliability by planning for redundancy in the network design.
- Consider the pros and cons of centralized network design vs. distributed network design.
- Consider additional services and the special requirements for business customers.

5. WISP management functionality and systems

5.1. WISP management systems overview

All telecommunications businesses are managed in a very similar manner even though their networks and delivery technology may be different. The telecommunications industry developed business management procedures and tools for companies that operated wire line phones (PSTN - public switched telephone network). Eventually the wire line companies added many other services, including Internet using DSL over the copper lines and later added fiber circuits. The phone companies also entered into the TV network business by streaming TV channels over the Internet network. The cable companies that began providing a TV network over cable also entered into the telecom business by adding Internet communications over the cable network and then offering telephone services. In parallel with these developments the mobile phone telecom companies first offered voice and later text services. The invention of the smart-phone allowed the mobile phone companies to add data services over the wireless connection. As these developments were happening there was a part of the population that did not have access to the phone network, the cable TV network or the mobile phone wireless network. The reason was mainly geographic, with people who lived in rural areas where the telecommunications companies decided it was too expensive to build infrastructure for this group of people. An opportunity was opened for entrepreneurs who began providing a wireless data service to part of the population that the telecommunications companies ignored and built the infrastructure with low cost wireless equipment that operated on unlicensed frequency bands. These entrepreneurs are the Wireless Internet Service Providers, WISP's.

The telecommunications companies of all types have a common set of business management requirements and WISP's have the same basic set of business management requirements as do the telecommunications companies.

- The customers are subscribers who pay each month for the communications service and so the company has a billing system to invoice customers each monthly billing cycle and collect the payments.
- The telecommunications company requires a sales data entry system to add new customer information and create a new subscriber database entry.
- A customer has to be provided with a copper, fiber or wireless circuit and equipment to connect to the circuit, which requires technicians to build infrastructure up to the customers location and install equipment at the customers premises, a process that is called provisioning. The company also needs a warehouse to keep a stock of the equipment that is required to connect the customers so that a new customer is connected very quickly.

- The telecommunications company communications network that requires constant configuration changes as the network expands to add new customers, and monitoring of communications errors that occur in the network, with maintenance work to optimize or repair the network.
- When a customer has a problem the telecommunications company has customer support staff to help the customer solve the problem, and if necessary make some repair at the customers installation. The customer support will also include a customer relationship management (CRM) service that permits the customer to login to a portal and get the information about the account, including reading past invoices and paying for future invoices.
- The telecommunications company has electronic routing that connects the customer to the destination that the customer requires. A subscriber's computer has an IP address and sends a message with a destination IP address to connect to a web server and that connection must be routed through the network.
- The telecommunications companies billing system monitors the customer account payment status so that the service that the customer contracted is provided only if the bill is paid up to date, if the customer does not pay then the connection is not made.

Telecommunications industry engineers developed a set of management processes and procedures that encapsulated the business requirements listed above. The processes and procedures were then built into the software that was used to manage telecom businesses. The management system concept that was developed was called OSS/BSS, which refers to Operations Support System and Business Support System. The functionality of each part of the OSS/BSS model is listed below.

The Operations Support Systems (OSS) for telecommunication services has the following functions.

- Network management, monitoring and reliability systems.
- Service fulfillment, including provisioning, activation and network inventory.
- Service quality assurance.
- Customer installation and service maintenance.

The Business Support Systems (BSS) for customer facing telecom operations has the following functions.

- Product management, service plans or tiers, terms and conditions of delivery.
- Order management; transform a customer order into fulfillment of service.
- Revenue management, subscriber billing and payment verification.
- Customer Relationship Management (CRM) that includes customer support.

WISP management systems follow the OSS/BSS model although operating at a smaller scale than the large telecommunications company systems, with fewer subscribers and with subset of management features. The OSS/BSS telecom business management principles are considered to be industry 'best practices'.

Those readers who wish to learn more about the OSS/BSS architecture and processes can consult the Telecommunications Forum (www.tmforum.org/oda/) where telecommunications business management methodologies are documented. The OSS/BSS model has been superseded by a new framework concept, however the business management objectives remain the same. The TM Forum's New Generation Operations Systems and Software (Frameworx) for the telecom industry is an evolution of OSS/BSS process design. The new framework has many features for telecommunications companies that have diversified into parallel areas of service.

The telecom management model is summarized in the following process diagram that illustrates the principal functions of billing, network management and customer care.

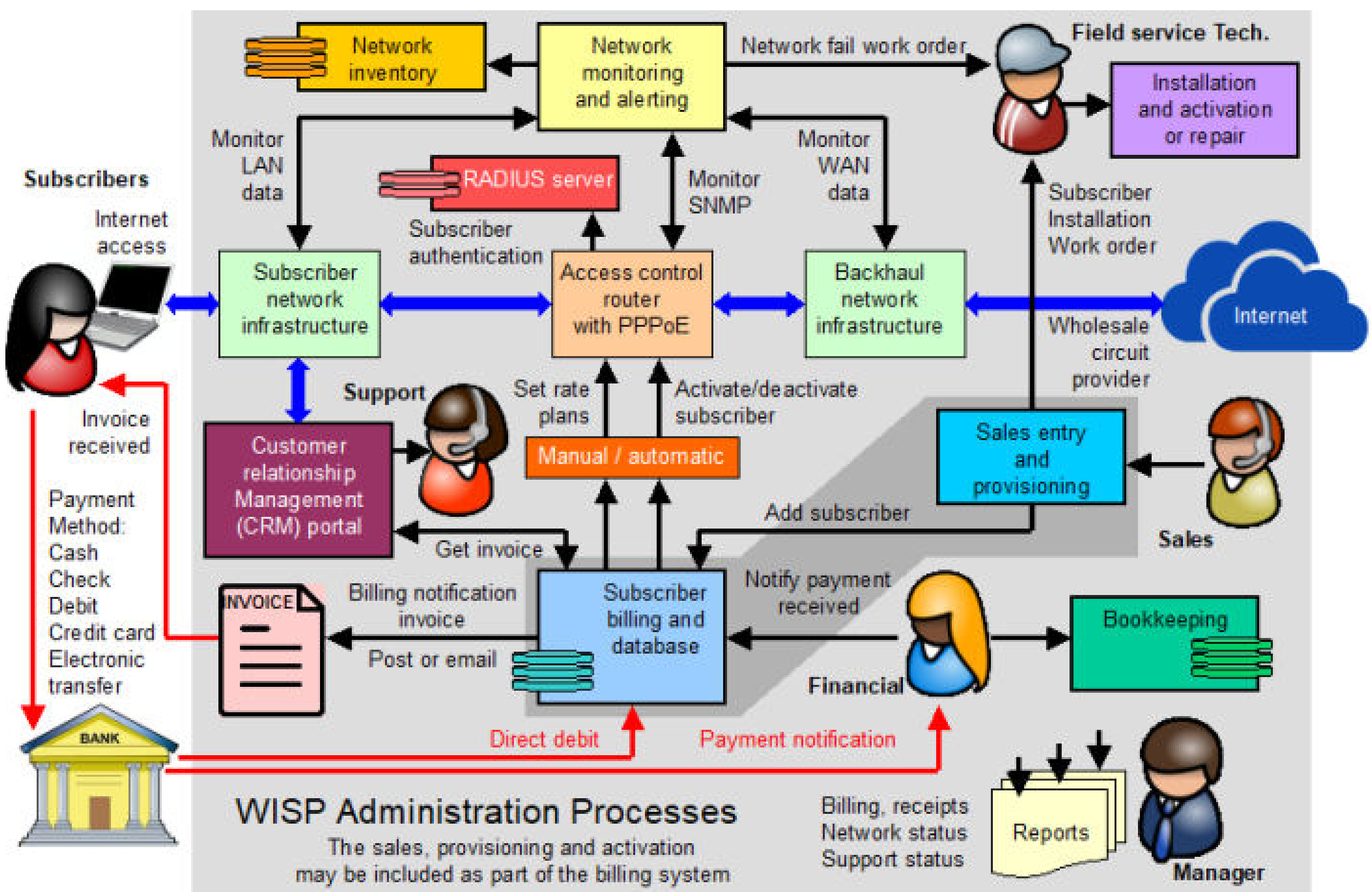


Figure 5.1.1. WISP management business processes.

The diagram has been simplified for clarity and does not include details of all processes required for business operations. The functions of sales, provisioning and activation can be incorporated within the billing system.

The subscriber connects to the Internet through a circuit that includes the subscriber network infrastructure (PtMP and PtP links), the NOC (access control) and the backhaul network to the wholesale access provider. The management processes ensure that the Internet service is delivered to the customer in a reliable manner with the rate plan that the customer requested, and that the customer is charged for the service at the beginning or end of the billing cycle, with a verification that the customer payment is received in a timely manner. Failure to pay on time will result in deactivation of the customer's service until payment is received.

The customer billing cycle starts with the sales person adding a new subscriber to the system. The customer should agree to a contract the service for a minimum period, usually 1-year. The customer will provide a billing address plus the method of payment. If the customer terminates early then the customer will be charged an early disconnection fee. The subscriber chooses a rate-plan; this is the type of service and the monthly charge for that service. The pre-pay subscriber pays for the monthly connection service before the start of the billing cycle. With post-pay the company gives the subscriber time to pay for the billing cycle after the end of the billing cycle, usually up to 30 days afterwards. The company also has a policy of charging the subscriber for the installation of the circuit at the subscriber's premises or else there is no charge for the installation but the company amortizes the cost of the installation over the minimum period of monthly payments with a higher monthly charge.

When the new subscriber information has been entered into the sales system it generates two outputs. First the subscriber information is added into the billing database and secondly a subscriber installation work order is initiated. The circuit installation to the customer's site is coordinated with the customer by the customer support staff and installed by the field service technician. Once the customer connection is verified to be functional then that date becomes the start date of the billing cycle. For pre-pay billing an invoice is issued before the start of the billing cycle each calendar month to request payment. The payment should be received on or before the billing cycle start date noted in the billing system. Some forms of payment such as checking account direct debit can inform the billing system directly via a gateway that payment has been received. The financial staff is also responsible for the bookkeeping, ledger, accounts payable and receivable, and payroll.

The billing system tracks the billing cycle of each subscriber and issues the invoice either before the start of the billing cycle (pre-pay) or else after the completion of the billing cycle (post-pay). The billing system can also have a third mode of payment, called on-demand, which is a pre-pay method. On-demand payment is not a monthly subscription service but a payment for a pre-determined length of time so that the customer can pay for Internet service when needed, and not pay when not needed. On-demand customers have the same infrastructure as pre-pay and post-pay customers. The on-demand payment method is similar to a public Hotspot service.

The billing system provides two items of information for the access control router; this is the rate plan (maximum download and upload speeds) and activation or deactivation according to the payment status of the account. There are two methods of programming the access control router. The first method is a manual operation where a staff member will take daily instructions from the billing system and program those instructions into the access control router. The second method requires a billing system with an API (application program interface) gateway to the router so that it can send instructions directly to the router. The second method is the preferred method of operation because business operations are simplified. In the case where the subscriber's payment is not received by the due date then the subscriber is deactivated by the billing system either manually or automatically until payment is received.

There are many different types of monitoring software available for the network monitoring and alerting module, some are free and some are purchased. Monitoring software can also be open source or proprietary. All have the same function to collect information from network devices using the Simple Network Management Protocol (SNMP) protocol; the differences lie in the method of displaying the information and the methods of analyzing the data for diagnostic purposes. The WISP configures the monitoring software with IP address information for each device in the network that contains an SNMP agent. Some monitoring software can auto-locate SNMP devices. The monitoring software periodically collects information from each SNMP based device. The frequency of the data collection is controlled by the WISP; too frequently will give a high data overhead on the network, less frequently will mean that any failure will take time before being recognized. The data collected from each SNMP device provides information about the status of the device and status about the data traffic flowing through the device. The monitoring software creates a database of all monitored devices with the status and other information displayed on the screen. This database is the network inventory that the administrator can view to check on the health of the network. The data that the monitoring software collects can be displayed in various formats. Some information is essential to verify bottlenecks in the wireless distribution network by observing a time varying graph of each circuit link throughput to evaluate if the link is operating at maximum capacity. If this is the case then the link has to be upgraded to provide a greater data throughput. The most important part of the monitoring process is what happens when the device does not respond to the SNMP request. Failure to respond means that the device has failed or the network connection to the device has failed. The software must generate an alert to the administrator who then creates a work order for the field service technician to repair the fault. Speed of response is very important, as customers will begin calling to complain about the loss of service.

The RADIUS (Remote Authentication Dial-In User Service) authentication software is required to verify that each customer is permitted to access the network. There are several methods of authenticating customers. A popular method used by WISP's is PPPoE (Point-to-Point Protocol over Ethernet) where the credential is provided by the CPE device and received by the PPPoE server, which is contained in the router. The router then forwards the credential to the RADIUS server for authentication. Once the subscriber is authenticated the data packets from that subscriber are transported over the network. Another popular and more secure authentication method is WPA2-

enterprise and is configured between the CPE and PtMP wireless. Each CPE has a unique credential that is passed to the PtMP wireless, which in turn forwards the credential to a RADIUS server for authentication. Once authenticated the PtMP wireless forwards the CPE data traffic over the backhaul circuit. Customers can be added manually to the RADIUS subscriber credential database, or else the billing software can send customer credentials to the RADIUS server database in order to automatically update the RADIUS credential register each time that subscribers are added to the billing system.

The customer relationship management (CRM) portal is a website subsystem that interfaces with the billing and customer support software. The customer can log into the CRM portal for access to billing information and to interact with the WISP customer support staff. When the customer first becomes a subscriber the customer receives a username and password account login to access information via the CRM portal. The customer can login to the CRM website portal even when the customer has been deactivated through non-payment. The CRM portal can include the following features.

- View the status of the account and data usage. Data usage is important if the account has a data cap.
- View paid invoices and download the invoices to print.
- View an unpaid invoice and make a payment online using a credit card.
- Open a support ticket with the support staff to ask any question about the account or the services that the WISP provides. The support staff member will respond to the question or else forward the question to another member of staff to answer.
- Request a change in the type of service contracted.
- Change personal information such as phone number or email address.

Additional features can be added as determined by the services that the WISP is offering. For example the WISP might offer a phone service using voice over Internet protocol (VoIP) or a streaming TV service, and may wish to provide information to customers about these services via the CRM portal.

In addition to the subsystems shown in the diagram there is also a marketing process that captures new customers and funnels them to sales through a qualification process. There are many software products that implement the sales and marketing process including cloud software. The most popular cloud software service is salesforce.com. The customer environment will determine the features of the sales and marketing process that the WISP requires. The WISP can add a customer capture component to the business website which funnels information to the sales staff for qualification. The WISP may have a retail store for walk in customers and so a PoS system is required.

The WISP has many software options that incorporate the management features to run the business, and can be divided into the following categories.

- Open source free software.
- Free software provided by equipment manufacturers.

- Software that is purchased and supported.
- Cloud software that is paid for by the number of subscribers.

Open source software is generally limited in the scope of features and requires good technical knowledge to install on a Linux server. The advantage of open source software is that the WISP who has programming skills can adapt the software for specific business requirements. Although the software is free there is a hosting operational cost. If the software is installed in the NOC then a server and backup up power is required. If the software is hosted with one of the cloud vendors then the operation will be reliable however the monthly hosting costs will increase as customers are added because more storage is required. An advantage of cloud hosting like AWS is that server capacity is not an issue; the host adds resources transparently as the processing requirements grow. Businesses that provide open source software also offer services to install and support the product.

Some WISP equipment manufacturers, like Ubiquiti, provide software to manage the business. The software packages are generally good but tie the WISP into the vendor's products, which is the objective of providing free software. In the case of Ubiquiti software there is no manual and no support form the manufacturer; the WISP has to rely on user groups to get information about the product. A high level of technical skill is required to install and configure the Ubiquiti software. There is a cost to host the software, either on the WISP's server, or on a cloud service such as AWS. The manufacturer may offer a free hosting service for the software however the network must be built with the manufacturers products to qualify for the free hosting service.

Software that is purchased and supported offers a good solution for a WISP entrepreneur whose technical skills are limited. Purchased software has more features then the free software and works with a range of different equipment; it is not tied to the hardware of one manufacturer. In addition to the purchase cost of the software there is also the cost of hosting the software, either on the WISP's server, or in some cases the software vendor will host the software for a monthly fee. The advantage of purchased software is that the monthly operating cost is not tied to the number of subscribers, unlike cloud systems.

Cloud software for WISP's is probably the biggest category of vendors. Cloud systems are popular because they require a minimum of technical knowledge to install and use, and are on the same ease-or-use level as bookkeeping software. Some cloud vendors provide a plug-and-play system that included the RADIUS server and have an API interface for popular routers, such as those manufactured by Mikrotik, to implement all access control functions. Although cloud systems are very easy to use they generally charge per subscriber, which many WISP's don't like because a percentage of the WISP's sales goes to the cloud vendor. Many cloud system vendors charge in the range of $1 to $2 per month per subscriber but it should be noted that this is for a comprehensive management system that includes billing with sales and provisioning, monitoring with authentication, and is plug and play so is very easy to install and use. A charge in this range is affordable for WISP's in North America who might be charging customers from $50 to $100 per month, however the charge may be too high for WISP's in emerging economies who might be charging customers less than $5 per month for a basic slow speed service. Emerging economies where entrepreneurs are building WISP services include Latin America, Caribbean, Africa, and Asia. The economic ability of WISP customers in emerging economies is much less than North American customers. Fortunately there are some WISP management cloud products developed for emerging economies that charge in the range of 10 to 20 cents per subscriber per month. The features are slightly fewer than the more expensive counterparts, but do include all management functions that the WISP needs. Cloud systems developed for emerging markets also include multiple language support for Spanish and other languages. In addition the low cost cloud management systems have inexpensive fully integrated redundant routers to implement access control and can also be integrated with low cost routers such as those manufactured by Mikrotik for lower cost but without redundancy. The use of a low cost cloud management system for the management of a WISP business is the subject of a later chapter in this book.

5.2. Service rate plans

There is no single service cost and data circuit speed that is appropriate for all customers. Some customers want the least possible cost for the Internet service and are satisfied with a slow data speed. Some customers want a fast data speed and can afford to pay for that service. There are also customers who seek a service at points in between these two extremes.

It is necessary to develop a range of service rate plans to offer a range of services that will meet the needs of all customers. Service rate plans are sometimes called service tiers. The service rate plan applies to both fixed broadband and mobile broadband customers. Both types of customers have data speed limits and sometimes data byte limits imposed. The difference between the two is that the fixed broadband customer has continuous service providing that payments are received and is charged monthly for the service, whereas the mobile broadband customer purchases a plan that has a limited duration.

The service rate plans that the WISP will implement depend on a detailed analysis of operating costs and research with prospective customers. Service rate plans can be adjusted as feedback is gained from the prospective customers and as more precise operating data is obtained.

Examples of service rate plans for fixed broadband customers are as follows.

- 5Mb/s download /500Kb/s upload speed, $10/month.
- 10Mb/s download /1Mb/s upload speed, $19/month.
- 20Mb/s download /2Mb/s upload speed, $35/month.
- 40Mb/s download /4Mb/s upload speed, $65/month.

Several data rate plans permit up-sell marketing to persuade customers to move up to the next higher price-tier to increase revenue per customer. It might be advantageous to incorporate a cost saving with increased speed increase as an incentive to persuade prospective customers to move up to the next tier, provided that there is a large data bandwidth available from the wholesale service provider. It is usually the case that the wholesale provider bandwidth is limited and so the guidelines of the contention ratio plan should be followed when offering bandwidth to customers.

For fixed broadband customers the service rate plan parameters are part of the customer record that is stored in the billing database. The WISP can change the customer's rate plan at any time in function of the customer wishing to pay for a faster data service or change to a lower cost data service. The typical service parameters that can be configured for fixed broadband customers are as follows.

- Set maximum download and upload speed limits.
- Optionally set the maximum download and upload byte count (data cap).

The fixed broadband management system will usually include a customer relationship management (CRM) portal where the customer can login and look at the status of the account, download past invoices and also open a support ticket. The billing system can be configured to suspend the customer's Internet access if the payment is not received by the end of the billing period.

Mobile broadband customers have similar service rate plans as those of fixed broadband customers with the addition of an access code duration value, which determines the length of time that the access code is valid before it expires. The mobile broadband customer rate plans are purchased on-demand as required. The rate plan parameters for mobile broadband customers are embedded into the access code that is printed on the voucher, which is sold to the customer. Examples of service rate plans (access code vouchers) for mobile broadband customers are as follows.

- 1-day duration, 5Mb/s download /500Kb/s upload speed, $2.
- 1-week duration, 5Mb/s download /500Kb/s upload speed, $10.
- 1-month duration, 5Mb/s download /500Kb/s upload speed, $30.
- 1-day duration, 10Mb/s download /1Mb/s upload speed, $4.
- 1-week duration, 10Mb/s download /1Mb/s upload speed, $15.
- 1-month duration, 10Mb/s download /1Mb/s upload speed, $45.

The service parameters that can be configured for mobile broadband customer on-demand charges are listed below. There are more variables for mobile broadband than for fixed broadband, and all are encoded with the access code. The time allowed to access the Internet is usually a fixed period, and there will also be other limits imposed.

- Time period that the access is activated for; e.g. 1 day, 1 week, 1 month, etc.
- Instruction to start the code period when first used and to provide Internet access until the period ends.
- Option to start the code period when first used and set the date at which the code will terminate.
- Option to stop/start the code to extend the time that the code will terminate on completion of the period.

- Set maximum download and upload speed limits.
- Optionally set the maximum download and upload byte count (data cap).
- Option to allow the customer to use the access code with one device or many devices when used serially.
- Option to allow more than one customer to share the same access code concurrently (shared code).

On-demand payments are required for mobile broadband customers but can be offered to fixed broadband customers if required to meet market conditions.

Customers have two types of services that determine how and when the payment is made.

- Pay monthly for a continuous subscription service; a periodic charge that can be pre-pay or post-pay, usually for fixed broadband but can also include a mobile broadband service. The fixed broadband customer is permanently connected to the Internet however in the case that the payment is not made the service is suspended.
- On-demand payment for limited time or data use as required, usually for mobile broadband but can be a method of charging for fixed broadband. The customer purchases a credential, which can be a token or voucher that gives Internet access for a limited period of time, or for limited data access, or both.

The methods of charging customers for the wireless broadband Internet service are determined by the payment services available in each country and the methods of payment available to each customer. Some prospective customers have bank accounts and credit cards that can be used for payments. Some countries might have prospective customers who do not have bank accounts or credit cards but can pay cash and so methods of receiving cash payments will be necessary. Some countries have cash payment systems where the WISP can receive payment via a payment network service. A summary of methods for receiving payments is listed below.

- Credit card payment for the monthly service.
- Bank check posted to pay monthly service.
- Bank account direct debit.
- Cash payment received at retail point.
- Cash payment sent over a payment network (e.g. Oxxopay in Mexico).

The WISP should implement several payment schemes that are convenient for customers who will be paying for the service.

Some payment methods are illustrated in the next diagram.

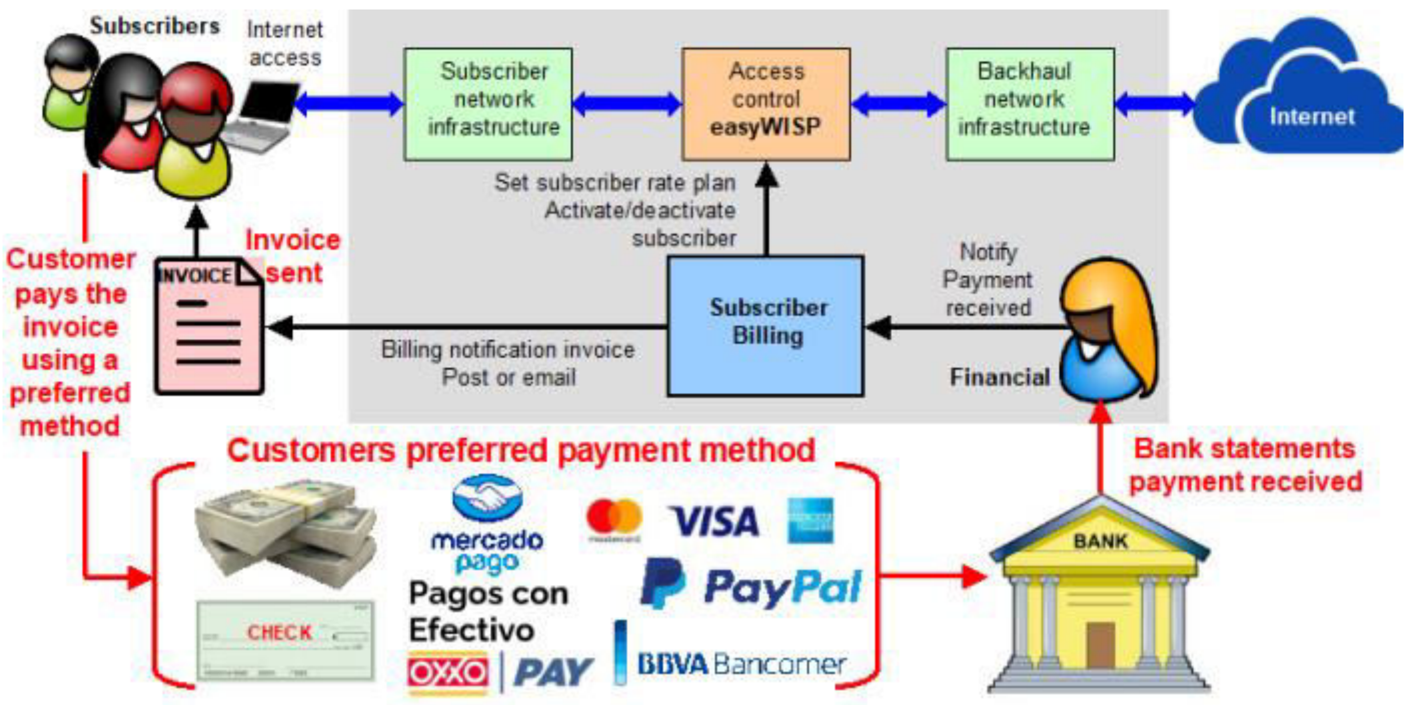


Figure 5.2.1. Service charge payment methods.

5.3. WISP staff roles

WISP management software assumes that the WISP has employees who function in several roles within the business. When an entrepreneur starts a WISP it is likely that the entrepreneur will assume all the roles in the business until the business is making sales. As the business expands the WISP will hire staff to fill roles within the business. A WISP business workload can be divided between five roles in a small organization.

- **Managerial**: responsible for management of the business, supervision of all roles, analysis of operational data, decisions about investments to grow the business, and acquiring investment capital to grow the business. Daily responsibilities include decisions about the subscriber billing rates, network planning, authorize purchasing, equipment investments, hiring and HR, and security and safety. Skills include managerial experience and technical knowledge of WISP operations.

- **Technical**: the field service technician follows work orders and is responsible for the installation of new subscribers, maintenance of existing subscribers, repairs and maintenance for the network, tower PtMP installation for expansion of the network, network monitoring and maintaining an inventory of parts for installations and repairs. Skills include computer operation, networking, fault location and repair. As the WISP business grows technical staff may be divided by function; for example tower installers, subscriber installers, network maintenance and repair.
- **Customer service**: The customer service staff is responsible to answer customer questions, which may come via the CRM portal, or a customer may call by phone, regarding problems, terminations, requests for upgrades, etc. Issues that customer service cannot solve are escalated to staff with the required skills. Skills include understanding business operations, friendliness and problem solving. Some WISP businesses may have a retail office that is staffed by sales and customer support staff.
- **Finance**: The responsibilities of financial staff are to maintain the billing system information up to date, receiving customer payments, entering customer payments into the billing system, and following up with late payments. Bookkeeping will include general ledger, accounts receivable, accounts payable, payment of expenses and commissions, collection and payment of communications service and sales taxes, and payroll. Skills include financial management and persistence with collection of outstanding receivables.
- **Sales**: responsible for attracting and acquiring new subscribers, adding subscribers to the billing system with data entry and editing, including entering the subscriber rate plan chosen by the customer (which determines the billing rate), up-selling to existing subscribers, and responding to subscriber questions about the service. Skills include negotiation ability, marketing creativity, and aligning rate plans with markets. The WISP might take advantage of specialized sales software, such as salesforce.com, that tracks prospects through the sales funnel to focus the sales and closure process.

The technical and sales roles can expect to employ multiple people as the business grows. Each new subscriber requires the field service technician to make an onsite visit to the customers premises to install the CPE wireless and the wireless router inside the premises. One field service technician may be able to install from 5 to 10 customers per week although that figure might be less if the technician is also extending the network and making network repairs. In order for the WISP to expand the business several sales people may be required to market the services, and qualify leads through a sales funnel to attract new subscribers. It is likely that for each new subscriber, the sales team may have contacted 10 to 25 people who enquired about the service.

The process model for WISP business management described in this chapter assumes the five employee roles listed in this section.

5.4. Management system processes

There are many different approaches to implement WISP management software. Most software is modular so that the WISP can manage the business with several stand-alone software products. The WISP software is divided into three subsystems, billing, network and CRM. The advantage of installing integrated WISP management software is that information is shared between the subsystems. The subsystem for work order entry, provisioning and activation may be included as part of the billing system. The software systems are reviewed in the following sections and the diagram shown below summarizes the interconnection of software subsystems.

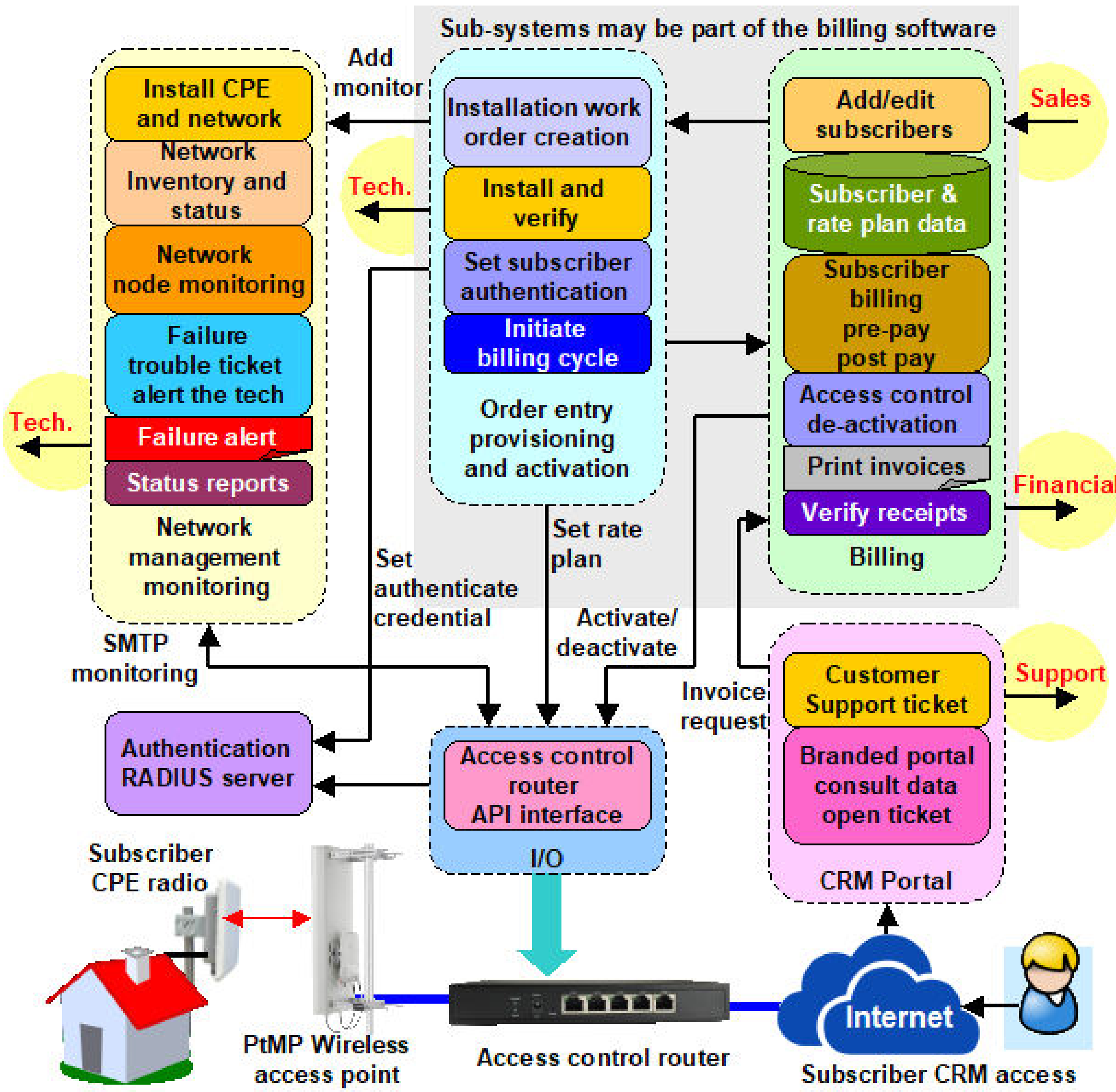


Figure 5.4.1. WISP management software subsystems.

- Subscriber billing: The billing software has a database that contains an entry for each subscriber, which includes the customer contact information, the billing payment method, billing cycle payment date and the rate-plan that was chosen by the subscriber. New customers are added to the billing database by the sales staff and it is necessary to initiate a work order for the customer installation. Financial staff issue invoices and note when payments are received, the software alerts when the payment is past due so that the financial staff can deactivate the customer until payment is received. Automated billing systems have an API interface with the access control router that will deactivate the customer when the account becomes past due. Billing can be configured for pre-pay or post-pay, and some billing systems also support an on-demand payment scheme. The billing system will provide management reports showing customer payment status, list late payments and show month-by-month revenue. If it is necessary to change subscriber information in the billing database or remove a subscriber then customer support may complete this task.
- Order entry, provisioning and activation may be included as part of the WISP billing system or else provisioning and activation can be separate processes. Information about new customers that was entered into the billing system with the sales order entry process can be read or downloaded and used to prepare a work order using a software or spreadsheet form. The work order will instruct the field service technician to install the customers CPE and network equipment then activate the customer. With manual access control router configuration the field service technician will enter the customer information that includes the rate-plan data into the access control router. Alternatively the billing system will have an API interface to the router and will install the customer information directly. On completion of the installation the technician will activate the customer to access the Internet and after the customer has accepted the service the technician will ask the customer to sign off on the installation and enter the start date of the billing cycle into the billing system.
- Network monitoring and failure alerting: the SNMP monitoring software is configured to fetch data from each device that has an SNMP agent, display that data in a consolidated format, and alert the administrator when a device does not respond to the SNMP request. With most monitoring software the WISP staff have to watch for the failure alert and create a work order for a field service technician to make the repair using a spreadsheet form or work flow software. Some monitoring software will send out an automated text message or email when a failure occurs and this information can be formatted as a work order for the field service technician. The network monitoring software will maintain an inventory of monitored devices and display the status of each device.
- Customer relationship management (CRM): the CRM software provides a portal for each subscriber to login to the subscribers account permitting the subscriber to access information about the account and billing status, and also make an on-line payment. CRM systems also provide a support ticket feature that permits the customer to open a ticket and send a message to the customer support staff. If the CRM system has an interface with the billing system then the customer can

request copies of past invoices or pay an open invoice online. The CRM system requires some branding and customization work to provide invoice and payment services for customers. The CRM software can generate a management report showing customer support tickets, including tickets that have been resolved and closed, and tickets not closed owning to dependence on some business factor. The manager can then follow up with staff to ensure customer satisfaction.

The starting point for the WISP management system process begins when a subscriber is added as a customer record to the billing database. The billing cycle can only start then the subscriber has been installed and activated. Adding a subscriber initiates the work order process to install the customer CPE and network. The field service technician goes to the customer's premises and installs the equipment then configures the authentication credential into the subscribers CPE device. The RADIUS server verifies the authentication credential when the customer connects to the network. The technician verifies that the Internet connection is functional and the subscriber is activated. When the subscriber signs off on the installation the technician initiates the subscribers billing cycle. Finally the technician adds the subscribers CPE device into the monitoring database for subsequent performance and failure monitoring. The network monitoring system will test each piece of equipment periodically and post an alert for any device that has failed to respond. Subsequently an invoice is generated for the subscriber at the start of each billing cycle interval. The WISP decides if the billing cycle is pre-pay or post pay when configuring the system. The billing system may also have on-demand billing where the customer pays for a specific duration of access or a quantity of data. The customer can login to the CRM portal to access information about the account, check paid invoices, pay an outstanding invoice or open a support ticket. The process flow is summarized by the following list.

- Initially create and configure the customer rate plans, brand the CRM portal.
- Order entry: A new subscriber entry is created in the billing database.
- Provisioning: The subscriber information creates a work order for installation. Configure the access control router for the new customer data then install the customer premise equipment.
- Activation: The subscriber is enabled to use the Internet service after installation and the billing cycle is initiated, the subscriber’s equipment is added to the monitoring database.
- Billing: Customer invoices are issued before the start of each billing cycle, past due payment will disable the customers Internet access. An on-demand payment mode is optional for subscribers and anonymous (Hotspot) users.
- Network monitoring: maintaining an inventory of network components and status log for each, a failure detection will issue an alarm.
- Reporting: network inventory and usage, subscriber list, outstanding tickets for customer support, failure alarms, billing receivables, accounts past due, and collections.
- Customer Relationship Management (CRM): account status, access invoices, open customer support tickets.

Some software manufacturers combine the software subsystems described previously so that they are integrated into one WISP management product. Having one software system instead of using two or three software products to manage the WISP business simplifies operational management. Some integrated WISP management software products include automation by implementing an API interface that will communicate with one or more access control routers and program the routers directly with the customer identifier, rate plan and activation information. A simplified process flow diagram for an integrated WISP management software system is shown in the next figure. This diagram illustrates all the basic functions that a WISP requires to manage the operation of the business.

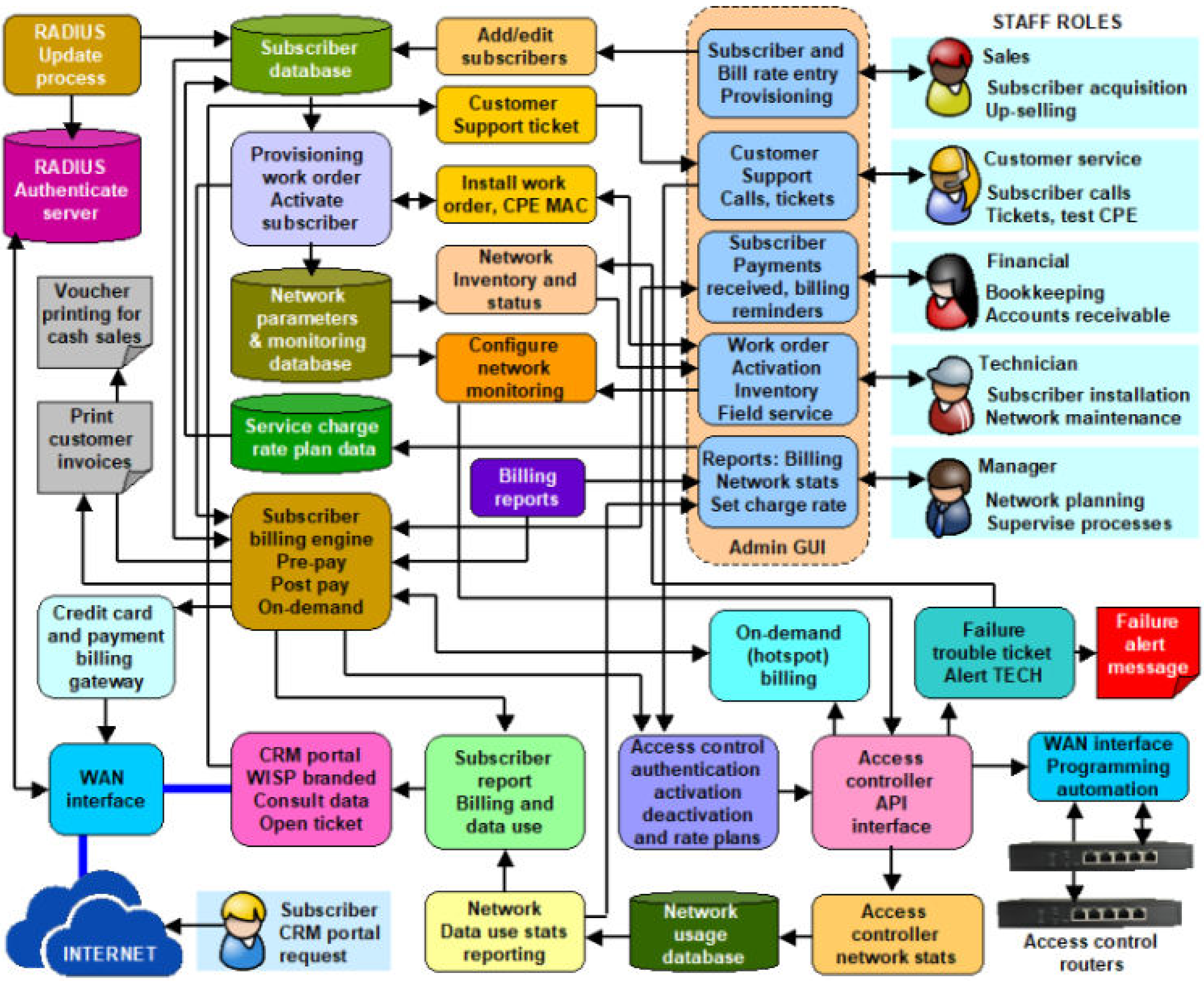


Figure 5.4.2. Integrated WISP management software system simplified process flow.

The WISP management system has a graphic user interface (GUI), which provides a secure login for five different roles of the WISP's business staff. The roles described previously are the manager, technician, financial, sales and customer support. The manager has access to all functions of the system. Each staff member has access only to those subsystems necessary for the staff member’s job function for added security. The manager will constantly supervise the operations to ensure that new customers are installed quickly and that any customer problem is resolved immediately to ensure customer satisfaction.

Initially the manager will set the subscriber rate plan billing rates in the service charge database. The rate plan is selected by the customer and is added to the subscriber database entry; the data speed setting for each customer is programmed into the access control router while the charge setting is used by the billing system to add the charge to the invoice. The manager will also decide if customer will pre-pay or post-pay each billing cycle. The manager will also decide if an on-demand payment service will be provided for customers.

Each time that the sales staff acquires a new customer the billing and address information is added to the billing system data entry together with the rate plan that the customer has chosen. The sales staff takes the first payment from the customer at this point. The payment can include the CPE installation cost and the first month of pre-paid service. The sales staff or automated provisioning module then takes the new customer data and creates a work order for the technician to initiate the customer installation process. The customer support staff answers any questions that the customer has.

The provisioning process will take the customer data and create a customer installation work-order, which is provided for the field service technician. The field service technician will prepare the subscriber installation kit with inventory parts and schedule a customer site visit directly or via customer support for the installation. The CPE information and authentication credential that will be installed for the subscriber must be configured in the RADIUS server. This can be a manual process or may be automatically programmed via a billing system that includes the RADIUS server. The customer identifier and rate plan is programmed into the access control router either manually or automated with a billing system interface communicating with the router API. The CPE information can be added to the monitoring software at this point but not activated until the CPE is on-line. If the processes are automated then the customer installation and activation process is simplified.

The financial staff handles customer billing, invoicing, collections and confirmation of payment. If the subscriber account is past due with an automated billing system then the billing system will communicate with the access control router API to deactivate the subscriber until payment is received. If not automated then the financial staff will open a work order for a technician to deactivate the subscriber through manual programming of the access control router.

The field service technician will travel to the customer's premises to install the CPE wireless and network equipment. After installation of the equipment the technician verifies that the authentication credential allows the CPE to access the network. With the device activated and accessing the Internet the technician has the customer sign off on the installation then completes the last two tasks; one is to initiate the billing cycle on the date of customer acceptance, the second is to activate the monitoring of the CPE and any other SNMP devices in the customers network.

Once the billing cycle has been initiated then the billing system is used to generate the customer's invoice for payment either before the start of the billing cycle (pre-paid) or at the end of the billing cycle (post-paid). Receipt of the customer's payment is notified to the billing system, either automatically via a gateway that is linked to a payment system, or else the notification is manual made by the financial staff. The financial staff will verify that the customer's check or other form of payment has cleared in the business bank account. If the billing system is not notified of payment then the subscriber will be de-activated and will loose access to the Internet. If the system has an automated API interface to the access control router then the billing system can deactivate the customer directly. If there is no automation then the financial staff advise the technician who then changes the customers setting in the access control router to deactivate the customer.

The access control router is configured to show a captive portal page to the customer who has been deactivated advising that payment has not been received. The captive portal page should provide access to the CRM portal so that the customer can pay the outstanding invoice on-line. The billing system can have access to a credit or charge card gateway, or a direct debit gateway so that subscribers who elect to pay by an automatic method can be charged for the service. When the customer payment is received after a late payment deactivation then the customer is reactivated, optionally with a new billing cycle start date.

The billing system may have an on-demand (Hotspot) billing option also as part of the billing subsystem. On-demand customers can purchase Internet access using credit cards or by purchasing access vouchers using cash. The vouchers are created and printed by the billing system. On-demand vouchers for cash sales are a popular method of selling Internet services in developing economies. The financial staff prints vouchers. The rate plan parameters are selected when creating the voucher; for example the duration of the code and the maximum download and upload speeds.

The billing system generates reports for the manager showing monthly receipts and also listing payments that have passed the due date. The financial staff will follow up with past due payments.

The monitoring software can verify the connection each subscriber and in the event of a connection failure an alert is generated. A field service support request is created for the field service technician who will then repair the problem that caused the connection to fail. A service report should be available for the manager to inspect. The monitoring software constantly gathers network traffic statistics from each data link and stores the data in the network usage database. The principal use of this information is to provide the network manager with a diagnostic tool to evaluate link conditions, and to identify links that are working at capacity and need upgrading. The manager may also wish to make adjustments with the tower contention ratios when a tower backhaul is under utilized. The customer support staff requires a software tool to test the circuit through to the customers CPE when the customer calls to complain there is no Internet connection. The test permits the support staff to initiate a work order for the field service technician if there is a fault connecting to the CPE, or else if the circuit is good then advise the customer that the fault lies in the network installed at the customers premises and there will be a charge for this repair.

The branded Customer Relationship Management (CRM) portal is a service provided for subscribers. Each customer receives a login credential to the CRM portal when the customer's account is created. The customer can login to access account information and make changes to personal information, access and open past and current invoices, and make payments on-line.

The differences between the small-scale WISP management system and the larger scale systems implemented by the telecom companies lies with the degree of automation, facilities for integration with external gateways for payment processing, and additional features to manage a broad range of service products, such as a telephone service or a streaming TV service. The large-scale management systems automate processes that the small WISP has to do manually. A high level of automation is not practical for smaller WISPs due to the cost and volume requirements to set up gateways with all banks and the financial processing services. WISPs in developing countries will have subscriber's who don't have bank accounts or credit cards, and so the WISP may have a retail point where subscribers will pay cash. The WISP can also use cash payment systems provided by 3rd parties; the transaction processing systems will vary from country to country and be subject to local laws.

The software subsystems are described in greater detail in the sections that follow. Before making a decision about software acquisition the WISP should carefully study each software manufacturers product in order to understand how the manufacturer has implemented the essential business process features required to manage the WISP business.

5.5. Order entry, provisioning and activation

Some parts of the subscriber order entry, provisioning and activation subsystem may be included with the billing system in most software implementations. The subsystem is described in this section for clarity because most software requires the WISP to implement some parts of the provisioning and activation process using several software such as spreadsheets and software provided by equipment manufacturers. A few integrated WISP management software systems do include all functions described in this section.

Before beginning to offer Internet services to potential subscribers the startup WISP must make decisions about how to install the service for the client, the installation charges, and the terms and conditions of the ongoing service. Some alternatives of installing the service for the customer are listed below:

- Determine if the WISP will offer customers a pre-pay or post-pay charging system. The pre-pay customer will pay before the start of the billing cycle; the post-pay customer will pay after the end of the billing cycle.
- The WISP has to decide if the new subscriber should be charged the cost of installing the CPE and other equipment and if the subscriber owns the equipment.

- The WISP can install the CPE and other equipment without charge, then charge the subscriber a monthly fee for rental of the equipment; in this case the WISP owns the equipment.
- Charge the new subscriber for installation services but not for the equipment, and charge the subscriber a monthly fee for rental of the equipment; the WISP owns the equipment.

The following diagram illustrates the sub-section of the WISP management system for customer order entry, provisioning and activation.

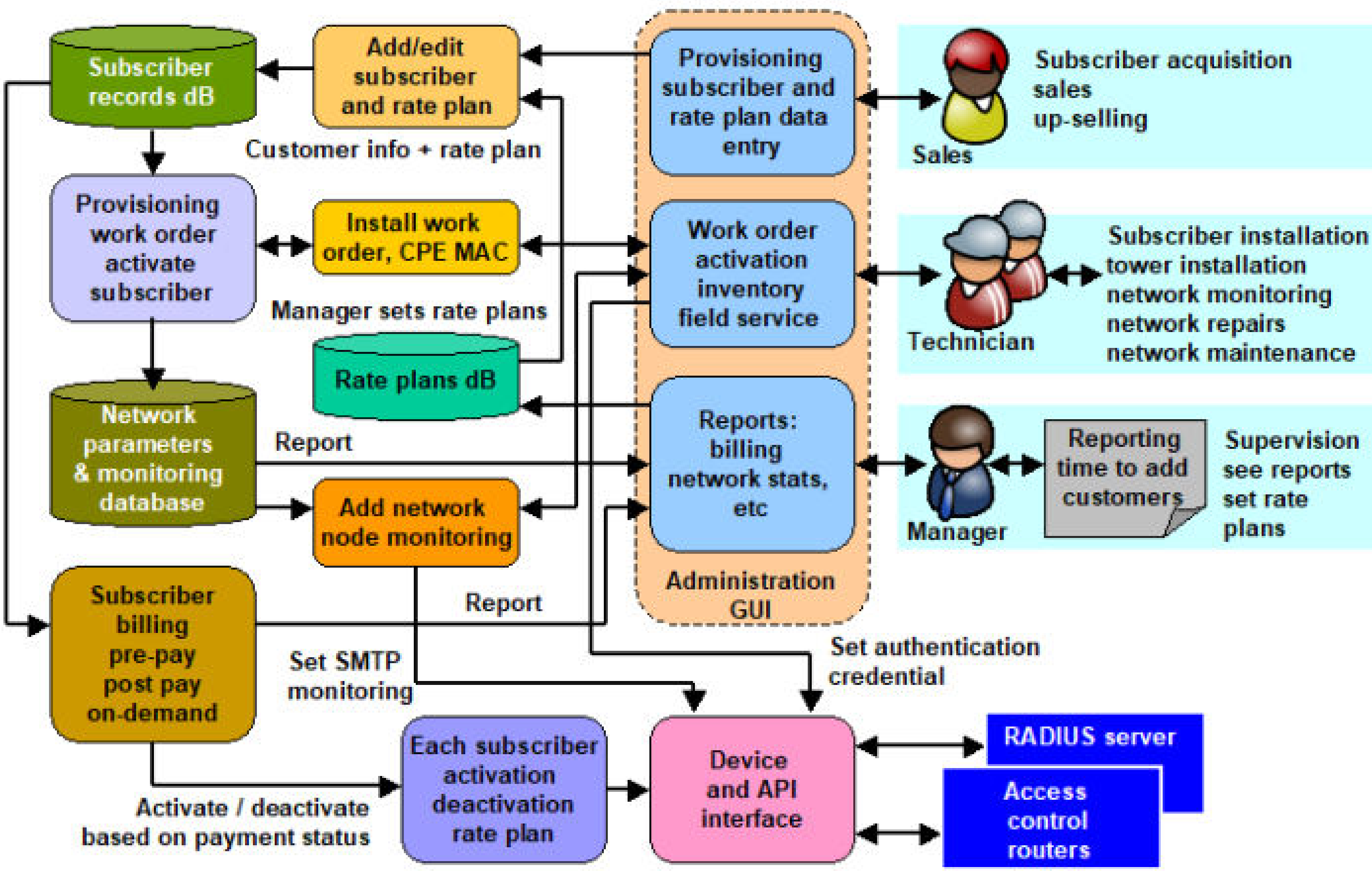


Figure 5.5.1. WISP Management subsystem, order entry, provisioning and activation.

The provisioning process follows after customer data entry. Customer data entry is used to add a new subscriber, modify an existing subscriber by updating personal information, and inactivating a subscriber who does not wish to continue with the service. When a subscriber is inactivated the contact information should be kept for future marketing purposes. The subscriber database is a valuable resource for marketing new services and upgrades to existing services and can reduce the cost of subscriber acquisition.

Before beginning the customer data entry process the sales person must verify two parameters that are essential for the successful installation.

- The first parameter that must be verified is that the customer’s location lies within the coverage area of the PtMP tower.

When the sales person has the first contact with a potential new customer it is important to ensure that the subscribers residence or business can communicate with the WISP's PtMP tower. When the tower was constructed the WISP should have drawn up a map, described in an earlier section, showing the coverage area of the antenna. The sales person will refer to the map when speaking to the prospective customer. The WISP has several choices to prepare a map of the coverage area. One simple method is to travel around the vicinity of the tower measuring PtMP signal strength at various points, and extrapolating lines between the points. Alternatively there are vendors who sell software services that can plot the PtMP antenna coverage area onto a contour map of the terrain, when the WISP provides information that includes tower location and height, type and direction of antenna with gain, and the expected antenna transmission power (ERP). The WISP will pay a fee or subscription for use of the software service.

- The second parameter that must be verified is that the CPE antenna can be installed at a high point on the roof of the premises.

It is possible that the customers’ building has some restriction regarding the antenna installation. This could be a home located in a condominium where the association has rules about the installation of antennas, or a rented office building where the owners permission is required to install the antenna, or similar. The prospective customer may have to produce written authorization to allow the antenna to be installed. In addition there may be municipality and zoning laws that require the WISP to pull a permit in order to install an antenna. The WISP should be aware of the local rules and regulations in order to avoid problems later.

The subscriber data entry, provisioning and activation subsystem may have a graphic user interface (GUI) that is used by sales staff to add subscriber installation information, billing information and rate plan. Typically the information that will be requested from the new customer and entered for the customer record is listed below.

- Subscriber name.
- Installation address for the CPE wireless and network equipment.
- Billing address if different from the installation address.
- Contact telephone.
- Contact email address.
- Username for the subscriber to access the CRM portal, this can be the subscribers email address. The password can be given to the subscriber or generated by the subscriber the first time that the CRM portal is used.

- Start date for billing cycle, this should be the date of activation and service acceptance by the customer; this is entered later by the installation technician.
- Tower PtMP radio, which will service that CPE address. The line-of-sight (LoS) between the CPE and the PtMP tower must be verified before the WISP can accept the subscriber for service.
- Rate plan selected by the subscriber, the maximum data down and up speeds, any data cap, and the monthly charge for the service.
- Monthly payment method, cash, credit card, check, etc.
- Monthly payment type, pre-pay, post-pay. This may be pre-configured in the billing system and not an option.
- Installation payment if applicable, or else the cost of installation is amortized with monthly payments.
- Name of salesperson making the sale, for a subsequent calculation of the sales commission.

On completion of the customer data entry the customer will sign a copy of the terms of service agreement and be given a copy of this document. The sales person should also print a receipt of the initial payment and give to the subscriber. The receipt should include the customer’s installation and billing information for the customer to check and confirm, plus statement of payment and taxes that were collected. After completion of data entry and receipt of payment the customer is now a subscriber and will make a payment each subsequent month corresponding to the start date of the billing cycle.

When the new customer data entry is completed a sequence of events that result in subscriber activation are initiated. First a work order is generated with a request to install the new customer CPE wireless and sent to the field service technician. The technician will add technical information to the work order such as the MAC address of the CPE device that will be installed at the subscriber's premises and any authentication credential that will be programmed into the CPE. The CPE MAC address may be part of the authentication process to allow the subscriber to connect to the network. The technician will also identify the PtMP tower that the CPE will connect with during the installation process. The access control router that will service the PtMP tower must be configured for the new subscriber. This may be an automated process where the billing system has an interface with the router API, or else the technician will program the router manually with the subscriber identification and rate plan information. Next the technician can add the CPE device SNMP agent to the monitoring software database, however the IP address of the CPE will be updated at installation when this information is available. The IP address depends on the IP allocation plan that the WISP has implemented. Each CPE device can be configured with a static public IP address (IPv4) if the WISP has public IP’s available. As IPv4 IP’s are no longer available the WISP will most likely configure the customer CPE with a private range Ipv4 address and optionally a public range Ipv6 IP address. The CPE device can also be configured as a DHCP client with the access control router configured as the DHCP server for the CPE and other network devices.

When installing the CPE to connect with the PtMP tower the technician will consult the MAP previously prepared by the WISP showing the area of coverage of the tower, and verify that the customer's location is well within the area of coverage. If the customer is located on the fringe of the coverage area it may be necessary for the technician to visit the location in order to verify that the CPE has unobstructed LoS to the PtMP tower. If the technician goes to the site but does not find LoS access to the PtMP tower then the customer's account must be cancelled and a refund made.

The customer support staff will negotiate the installation date and time with the customer then add this information to the work order before sending to the technician. The customer has to be present during the installation, as the technician requires access to the premises to install the CPE Ethernet cable and power supply, and the wireless router inside the premises. On the appointed date and time the technician will visit the site to install the CPE antenna and wireless router at the subscriber's premises. The technician must install the CPE on the roof of the building with a clear view of the PtMP antenna and so it may be necessary to have prior authorization to access to the roof of the building.

When the field service technician visits the customer premises to begin the installation the technician should carry all tools that are required for the installation; which will include power tools and test equipment. The technician should check the electrical voltage and ensure that the circuit is earthed. The installer will also have a laptop computer to configure the CPE and wireless router, and to check the connection to the PtMP tower. The technician will install the antenna on the roof of the building then run an outdoor Ethernet cable from the CPE inside the building. The CPE is powered over the Ethernet cable using the PoE supply. The CPE is then connected to a wireless router to provide Internet access for the customer.

To start the activation process the authentication credential is programmed into the CPE followed by verification that the connection to the PtMP tower is functional. After the functional test the technician will give the customer the WPA2 key for the wireless router, which should also be on a label attached to the wireless router, and request the new subscriber to check the connection. Finally the customer can sign off the work order agreeing that the installation is complete. The technician can then set the start date of the billing cycle and activate the device monitoring through remote access to the management software. With the activation process completed the technician will return the signed off work order to the WISP administration for archiving together with the terms of service agreement that the customer signed when the sale was made.

After configuration the customer will be billed for the subscription every month on the day corresponding to the start date. If the customer does not pay the monthly invoice by the due date then the customers Internet service is deactivated. If the billing system has an API gateway to the access control router then the billing system can deactivate the customer, if not then the technician will deactivate the customer manually as advised by the billing system.

The reporting interface of the WISP management system should permit the WISP owner to create reports that will help to analyze the results of the business. Some WISP management systems may permit subscriber data to be downloaded in comma-separated-value (CSV) format. The CSV data can be loaded into a spreadsheet, which the WISP owner can use to create reports. The following reports are desirable as part of the provisioning system and are useful for the WISP owner to help measure business performance;

- Subscribers joining, month-by-month, with annual total.
    - Calculate the average subscriber acquisition cost, sum the total sales and marketing costs for the month divided by the number of subscribers.
- Subscribers leaving, month-by-month, with annual total.
    - Follow up with each subscriber to discover why each left the service.
- Analyze subscribers per sales person to measure sales performance, month by month, with the annual total.
    - This report will be used to identify the best performing sales people. It may be necessary to adjust sales commissions to encourage sales efforts.
- Analyze the rate plans that are selected by subscribers as follows.
    - Are rate plans mainly low cost? Is it necessary to add even lower cost rate plans?
    - Are the majority of rate plans chosen for fast data speeds? Is it necessary to add faster data speed plans?
    - Are rate plans chosen in the middle range? Is it necessary to add more middle range rate plans?
- Identify marketing programs that are designed to increase the revenue per subscriber, increase the number of subscribers and maintain existing subscribers;
    - What up-selling incentive can be given to subscribers to persuade them to move up to the next higher priced rate-plans?
    - What referral incentives can be given to existing subscribers to persuade them to bring a new customer?
    - What loyalty program incentives can be given to existing subscribers to maintain them as happy and loyal customers?

Each WISP owner will have an opinion about the data that is important to manage the business and assess the business performance. It is important that the information the WISP owner would like to see can be extracted from the WISP management system.

5.6. Customer billing

There are a number of billing software products and cloud based billing services for WISP's. A list of software and cloud providers is included in the references at the end of this book. There are a few integrated software products and cloud services that combine billing with order provisioning and network monitoring. WISP's can acquire several software packages to implement all business management functions however there will be difficulties to integrate and share the data of each.

All WISP billing systems, both software and cloud, follow a similar functional model, which is described in this section, however they differ in operational details. A simplified process diagram of a WISP billing system is shown in the next figure. The description of billing system operation will refer to this figure in order to explain the billing process flow.

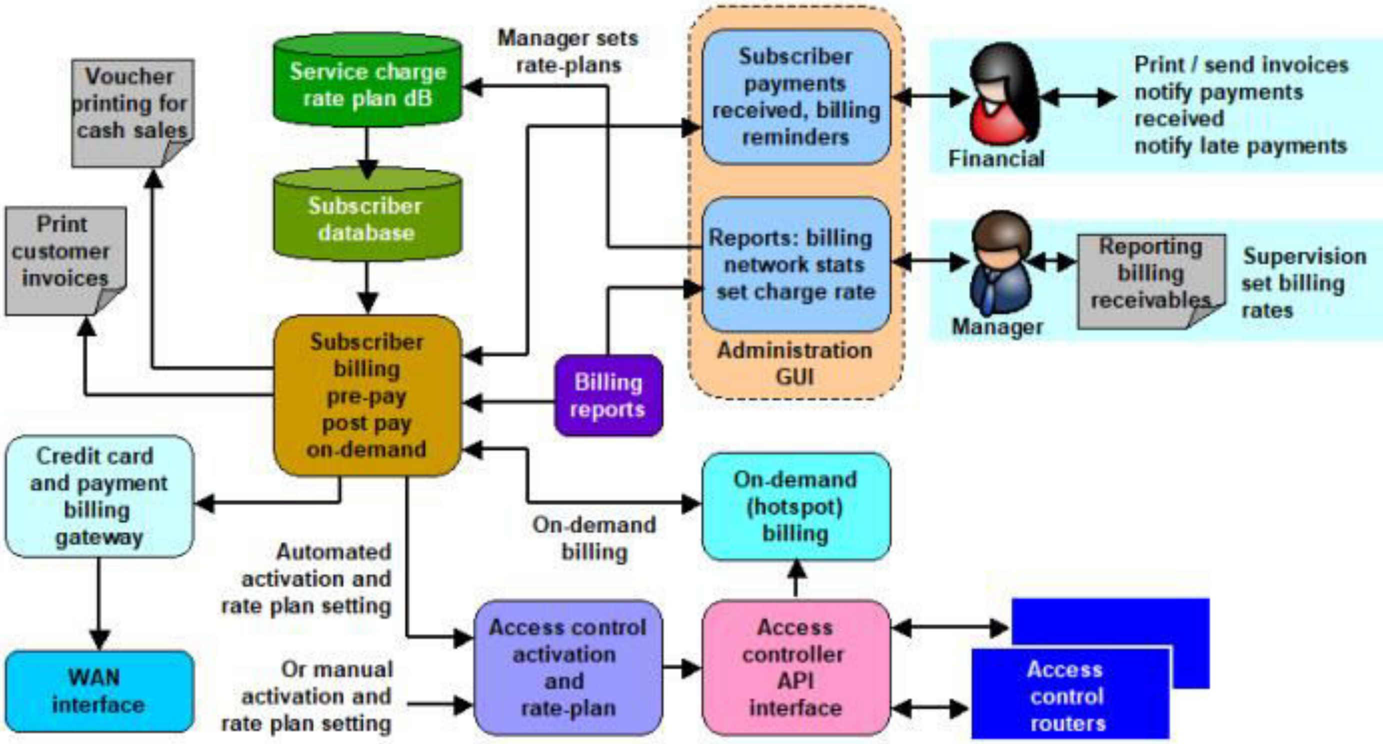


Figure 5.6.1. WISP Management billing subsystem process model.

When making a decision about purchasing or leasing billing software, or making an agreement with a billing cloud service provider, the WISP should consider the following alternatives.

- Free open source billing software.

Free open source billing software has no cost to acquire and operate the software however there is a cost to host the software either in the NOC or else using a cloud hosting service like AWS, and there is a cost if the WISP requires support from the vendor.

- Free software provided by an equipment vendor.

Ubiquiti is one example of a WISP equipment vendor that offers free software that can be used by any WISP. The software has no automation and so configuration of the access control router is manual, however the software has comprehensive features for billing, CRM and network monitoring of the vendors equipment. Ubiquiti will provide free hosting of the software if the WISP customer purchases and installs ten or more products from that vendor. Ubiquiti does not publish specifications or provide a manual for the software, and does not provide support. The WISP has to install the software and test all features to discover how the software works. The only source of support is the users group where users who have used the software share that information with others. This option is suitable for a WISP with advanced technical knowledge who can install and configure Linux servers and configure the software parameters, and who probably installs Ubiquiti prodcts.

- Purchase or lease billing software.

Software packages are available for WISP's that have full features and excellent support from the vendor. It is usual for the vendor to lease the software on a monthly or annual basis as few WISPs' have the money available for an initial large purchase. Software can be installed and hosted by the WISP as some WISP's with good technical skills like to be in control of the operations and don't trust cloud services, however there is a cost for hosting that includes servers and backup power. The software vendors will usually host the software for the WISP for an additional monthly fee.

- Contract with a billing cloud service provider.

Many WISPs' choose to work with one of the cloud service providers to get the billing functionality that the business requires. Cloud based billing systems have excellent features and the comprehensive coverage of business operations will satisfy the requirements of any WISP. Cloud based billing systems have excellent support and some provide automation providing an API for popular router brands like Mikrotik. The downside for most WISPs' is that the cloud service providers charge for the number of subscribers that the WISP has, with a charge in the range of $1 to $2 per subscriber per month. This charge is acceptable for WISP's in the USA where a customer might be charged $75 per month for a 50 Mb/s service, however the cost is extremely high for emerging economies where a WISP might be selling a 5Mb/s service for $5 per month. There are a few cloud service providers that target emerging economies and have a much lower cost of service with fewer features, which are nevertheless adequate for the WISP's business management requirements. Such low cost services are charging in the range of 10 to 20 cents per subscriber per month and also have multi-language product support. The WISP with limited technical knowledge is advised to start in business using a cloud billing service.

The WISP may have a strong technical background writing scripts for routers and is familiar with router products from Cisco and Mikrotik, and can configure them for access control applications. For the WISP's that don't have this technical background it is advisable to ask the vendor if the software or cloud service supports an API interface with a popular brand of routers such as Mikrotik to configure customers directly. Ask if the API interface will add a new customer authentication and rate plan to the router configuration and activate or deactivate the customer based on the account payment status. Ask also if the software or cloud service includes a RADIUS server for customer authentication and check that the billing system will update the RADIUS authentication database when new customers are added. The automation feature will simplify business management for the WISP and will permit the business to employ less skilled staff than would otherwise be necessary to program routers.

When the WISP first installs the billing software or cloud service the manager must install the rate plans that will be offered to customers. Each rate plan will specify the maximum download and upload speeds and the monthly charge for the service. The rate plan may also include a monthly data cap, which is important if the WISP is paying the wholesale provider for each GByte of data transferred. The manager can add new rate plans to the rate plan database at any time for salespeople to sell, however the manager should not change an existing rate plan as this will affect how existing customers receive their service.

The WISP has to be very flexible when billing customers and offer a wide range of payment methods. The WISP should have methods to received cash and checks and have a third party facility to charge credit cards and debit bank accounts. Some payment methods are unique to countries due to financial regulations. In Latin America for example, many people don't have bank accounts or credit cards but some countries have payment methods that permit the customer to pay cash at any retail store for an account such as a phone bill. It is usual for billing systems to offer several types of gateways to credit card processors, bank debit processors and payment methods such as PayPal. The customer will choose a payment method from those available and on the billing cycle date the billing system will charge the credit card or bank account for the monthly fee. If automatic payment methods cannot be used to bill a customer then the financial staff can issue a monthly invoice either via post or email to the customer. The customer can then post a check or use a cash payment method, such as using a cash payment processor or paying cash at the WISP's retail store.

Where the billing system has a payment gateway the billing system receives notification of payment and marks the account as paid. For other types of payments the financial staff will monitor payment methods daily, such as check deposits and bank account receipts and then set the customer account to paid.

In the case that the payment is not received by the due date then the WISP can suspend the customers service by deactivating the customer at the access control router. If the billing system has an API interface with the router then the billing system will deactivate the customer. If there is no API Interface then the financial staff must check the billing system each day for past due payments and then advise the technician to manually deactivate the customer using the access control router command line or GUI interface.

The billing system may also include an on-demand billing feature. This feature permits a customer to pay for a period of time or data volume of Internet access rather than be billed monthly for the Internet service. The WISP would prefer to receive monthly payments for a guarantee of cash flow, however on-demand billing is a payment method that will permit the WISP to sell Internet access to a customer who could not afford the monthly service or had only intermittent requirements for Internet access. The on-demand billing method can also be provided for anonymous users who are not customers but wish to use the Internet service for a short time. The WISP will have business customers who need on-demand billing for their customers. For example hotels must provide Internet service for their guests. A popular method of providing the Internet service is to provide a free low speed service then charge for a high-speed Internet service using a credit card. The WISP should have such an on-demand solution available to offer to business customers. There are several on-demand subscription services that provide Internet access in high-demand areas such as International airports.

The on-demand billing system generates an access code to authenticate a user, rather than using the authentication method that is used for subscribers. The on-demand mode of billing is also called Hotspot billing as it is used in many Internet Hotspot services. The access code is embedded with the rate plan parameters associated with the charge for the code as listed below.

- Duration of Internet access.
- Maximum download and upload speeds.
- Maximum download and upload data volume.

The access code can be purchased in the form of a printed voucher for a cash payment or else purchased on-line using a credit card. The billing system might include a feature to create access codes with the requested characteristics and then print the access codes on a printer in the form of vouchers. The vouchers are then sold for a cash payment. The codes can also be printed in the form of scratch-off cards by a specialized printing service.

The on-demand customer is authenticated using a captive portal login page that is programmed in the access control router using the captive portal feature. When a user connects to the access control router and there is no authentication record for that user then the user is re-directed to the login page display. The login page design is part of the CRM subsystem that the user sees to login to the customer CRM portal. The login page has a location to enter the access code that was previously purchased with a voucher, or else a button that permits an access code to be purchased. If the customer wishes to purchase an access code then that request is forwarded to the on-demand or Hotspot billing module in the billing system, which then forwards the customer to the credit card processor. On successful completion of the payment transaction the reply is returned to the on-demand billing module which then generates the access code for the customer with the embedded parameters that the customer chose at the time of purchase. The customer can then enter the login code to obtain Internet access. If the credit card payment processor declines the transaction then an error message is displayed on the login page stating that the payment was declined.

The billing system will provide a series of reports for the manager so that the progress of the business can be monitored. Billing reports can include the following.

- List of subscribers and payment dates and values, with sum total of sales for the past 30 days.
- List of subscriber accounts that are past due, showing days late for each.
- List of high data volume subscribers to sell upgrades.
- List of on-demand payments, a record of credit card transactions and the number of vouchers sold.

The sales staff should take responsibility for all customer issues, not only acquiring new customers, but should also follow up with accounts past due.

5.7. Network monitoring

Network monitoring software gathers information from the network components, using the SNMP (simple network management protocol) method. Network devices must have an SNMP agent so that they can be monitored, and the monitoring software is installed in the NOC (network operations center) or hosted on a cloud service such as AWS. Some of the integrated WISP management software systems will include network monitoring. Network product management uses software tools provided by the product manufacturers. Some products such as Mikrotik routers can be managed by software from other providers. The WISP manager needs frequently updated information about the network.

- How is the performance of the network? Where are the bottlenecks? Is network congestion occurring at any circuit link?
- Be notified immediately when an equipment failure occurs.
- Maintain a database of monitored products and show the status of each.

The network monitoring process described in this section can be implemented with one of several different SNMP monitoring software products, or can be a subsystem of integrated WISP management software that includes the network monitoring and failure alarm functions.

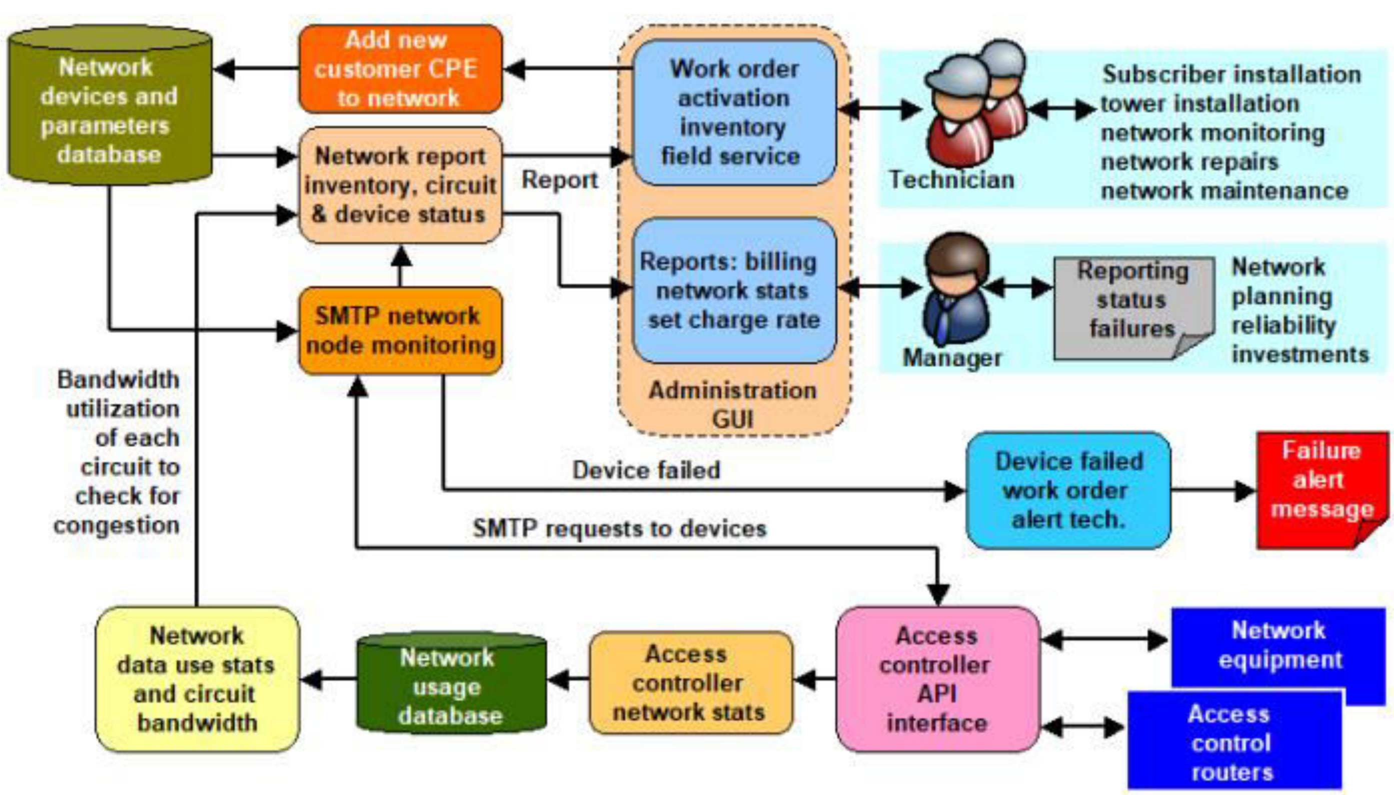


Figure 5.7.1. WISP network management and failure monitoring subsystem.

When the technician installs a customer CPE at the customer premises the device is added to the network database and SNMP monitoring of the device is initiated. The SNMP monitoring software will poll each monitored device in turn and collect the MIB data from each. The information is compiled into a monitoring report. If a device fails to respond to the SNMP request then either the device has failed or the circuit that connects the device to the network has failed. When failure occurs the network administrator is alerted and information about failure is compiled into a work order and sent to the field service technician to repair the network.

Data is gathered from each network device showing the data traffic over each link as a percentage of maximum capacity. This data can be logged and plotted as a graph with a time axis. This is important to view how much of the available bandwidth is being used in each circuit. If the link use is constantly at 100%, or at least 100% during peak hours then it is likely that network congestion is occurring. The monitoring data is compiled into a report by the technician who has a responsibility to monitor the data communications circuits. The manager should view the monitoring reports and is responsible to identify weak points in the network and make corresponding investments to improve the performance and reliability of the network. Network monitoring provides the information that can be used to prevent customers having a loss of the data connection. Failure monitoring will report a failure to the technical staff before the customers call to report a failure. Customer relations will benefit if the customer service staff can tell customers who call what the problem is and how long it will take to repair the fault.

There is one further requirement of the network monitoring system. Customer support staff should be provided with a tool to test the circuit connection from the NOC to the customer CPE wireless. This test is necessary because customers will call support to state that they have no Internet access. The customer support staff can then test the circuit to the CPE device to determine if the failure in the WISP circuit or a failure at the customer location. The WISP who is monitoring all CPE's for failure will know that a circuit has failed when the customer calls and can advise the customer about the repair process. The WISP should have a service schedule to charge a customer for a site visit when a repair is required to the network at the customer’s premises.

Network monitoring will provide reports for the manager to help make short-term and long-term infrastructure investments. A summary of reports is listed below.

- Inventory report of operational equipment showing the status of each device (on-line or off-line). The WISP should also maintain a second inventory of equipment in the warehouse that has been purchased to expand the network and purchased for subscriber installation kits but not yet installed.
- Configuration report of network equipment. If equipments permit to download the configuration then store a backup. If the equipment has to be replaced the backup configuration can be restored into the replacement device.
- List the monitoring alert failures that were detected and the corresponding work order that each failure generates. The manager should investigate (a) how the number of failures can be reduced through additional network investments, and

(b) calculate the mean time to repair (MTTR) and analyze how the MTTR can be reduced.

- Look at the bandwidth utilization for each data link and evaluate if the data traffic is using 100% of the data link bandwidth. If so plan a data link upgrade with more bandwidth or install a parallel link and use a load balancing router to share the data over two links, before network congestion occurs.
- Verify the circuit test to each CPE device and ensure that circuits are functioning as required. This is especially important if the CPE devices don't have SNMP monitoring.

5.8. Customer Relationship Management (CRM)

Customer relationship management (CRM) is an important part of the administrative processes. The purpose of CRM is to provide the customer with information about the account and to give the customer easy access to customer support staff. A satisfied customer will attract new customers. A process flow diagram of the CRM subsystem is presented in the figure below. Refer to this diagram for the description of the CRM operation.

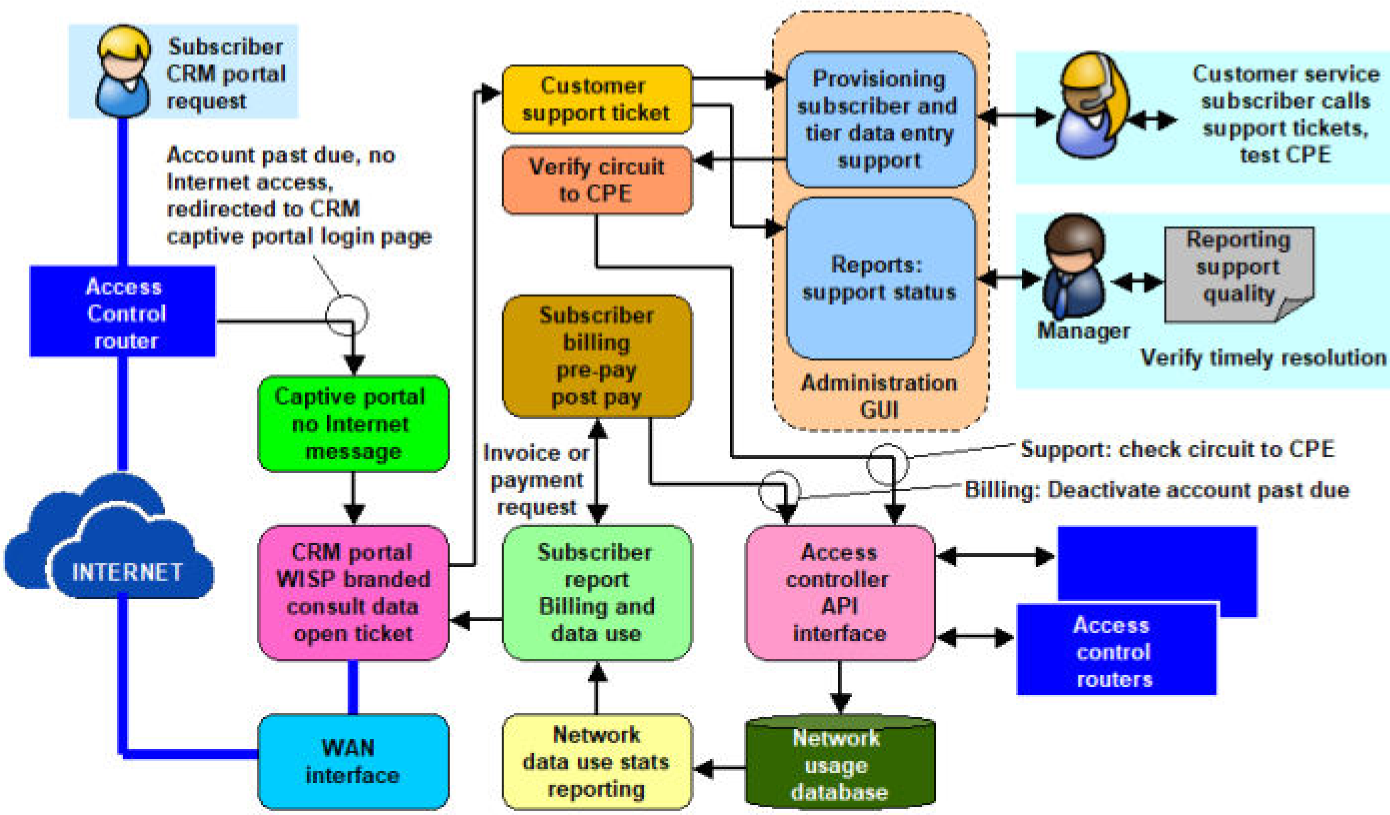


Figure 5.8.1. WISP customer relationship management (CRM) subsystem.

There are three reasons why CRM is important.

- Give each customer a channel to speak with customer support and catch problems before they escalate.
- Give the customer access to the account information, including historic data.
- Provide a marketing channel to customers for up selling, and can be used to build customer loyalty programs.

When the customer first becomes a subscriber the customer is given a unique username to access the CRM system and the customer then has to create a password. The CRM user interface (UI) can provide the customer with the following features.

- Check the status of the account, data usage etc. Data usage is important if the account has a data cap.
- Open paid invoices and download the invoices to print.
- Open an unpaid invoice and make a payment.
- Open a support ticket with the support staff to ask any question about the account or the services that the WISP provides. The support staff member will respond to the question or else forward the question to a qualified member of staff to answer.
- Request a change in the type of service contracted.
- Change personal information such as phone number or email address.

In addition the WISP can add marketing features to the CRM portal.

- Special offers to upgrade the account (up selling).
- Special offers for referrals (customer loyalty).

The CRM portal is also a user interface to on-demand access purchases.

- Login page that is used to purchase an access code using a credit card. The purchase will state the duration of the access code and the maximum data speeds.
- Login page to connect to the Internet by entering an access code that was purchased on-line or via a voucher.
- Location and information to purchase vouchers for cash payments.

To summarize, when the customer logs into the CRM portal using the username and password the browser displays the options available for the customer. The customer can look at data statistics for the account, which is fetched from the network usage database. The customer can also request copies of paid invoices, which are fetched from the billing system, or pay an outstanding invoice through the billing system using a credit card. The customer can open a support ticket with a request for information about the account. The support ticket is added to the support ticket list that is answered by the customer support staff.

The WISP can create categories of support requests via tickets of via phone calls. Most customers will make a phone call rather then login to open a ticket, as that is the process that people are accustomed to. A suggested classification for support calls is as follows.

- Service problem, request resolution, problem resolved.
- Upgrade service request, new rate-plan, add other service.
- Late installation, customer waiting as field service staff did not arrive at the date and time agreed.
- Service repair in progress, describe the issue.
- Service repair completed, get satisfaction report from the customer (1 to 5 stars).

If the customer calls the customer support staff stating that the customer has no Internet access then the customer support can test the circuit through to the customers CPE. If the test result is positive then the problem lies in the customers network. And the customer support staff can advise the customer how to proceed.

In the situation where the customer's bill is past due then the automated billing system will communicate with the access control router API to deactivate the customer's access to the Internet. When this occurs the next attempt by the customer to access the Internet will cause the access control router to redirect the customer's browser page to the CRM captive portal page, which will display a message stating why Internet access is not available and providing the customer with the opportunity to pay the invoice on-line using a credit card.

Some integrated WISP management software systems provide a CRM portal that is configured and branded by the WISP to provide the features that the WISP wants to offer to customers and a marketing area to promote the WISP's brand.

The CRM system provides reports for the WISP manager to monitor the performance of the customer support request resolution so that the effectiveness of the support system can be monitored. An important aspect of building a good customer relationship requires answering customer questions quickly and efficiently.

The manager should require customer support staff to keep a written record of customer calls. Customer support staff can also open a new customer support ticket when the customer calls by phone so that a written record of the call is maintained. The ticket will give support staff the opportunity to escalate the ticket to other members of staff, for example financial regarding a payment, or technical regarding a network problem.

A list of reports that the manager should obtain from the CRM subsystem is listed below.

- Access the ticket list (tickets opened by customers and tickets opened by support staff in response to calls from customers) to analyze the types of problems encountered by customers. Evaluate if it is necessary to make technical changes in the network or a business process change in the way that staff react to and solve issues that occur.

- Analyze the time taken to respond to requests and to close tickets on the successful conclusion of the issue. Evaluate what can be done to shorten the time to resolution (TTR) of each issue.
- Analyze the response to marketing via the CRM portal, how many responses were received, what are the results of the follow up process.

Good customer satisfaction depends on the degree to which the manager monitors the customer support process and takes action where necessary. Happy customers tell their friends about the great service and their friends then become customers.

5.9. Access control router management system integration

The functions and features of the access control router have been presented in earlier sections. In summary the access control router has the following list of functions that are programmed via command line or else programmed via the management software using the router API.

1. Store information about subscribers assigned to the access control router.
2. Configure one or more Ethernet connections to Interface one or more encrypted PtMP wireless access points that are connected via the wireless distribution network.
3. Authenticate the CPE device of each subscriber using an authentication method, one method will use the router PPPoE server and forward the authentication request to a RADIUS server.
4. Enable or disable access to the Internet of each subscriber assigned to the access control router based on the billing system payment status information.
5. Impose rules for the rate plan of each subscriber with regard to download and upload data speeds and optionally download and upload data caps.
6. Identify and report on link failures.
7. Monitor for attempted access by non-authorized devices, e.g. MAC duplication.
8. Inform management software of the status of the access control router via SNMP.
9. Operate autonomously providing access control for customers in the event that communication with management software is interrupted.

When the router has been programmed for the task of access control the router process determines how the customers data packet is managed. Each subscriber must have the account information programmed into the access control router, this information has been described previously and is listed below.

- Subscriber unique identification.
- Subscriber rate plan, maximum download and upload speeds, optional data cap.
- Subscriber enable /disable status determined by the payment status.

The information for each subscriber can be programmed using one of two methods;

- Manually using the router command line or graphic user interface (GUI).
- Programmed by the management software via the router application program interface (API).

The figure below illustrates the router processes when programmed for access control. The external interfaces to the router are identified, however all interfaces will communicate through one router Ethernet port that is used for control. The control port should be isolated from the network carrying customer data traffic for security purposes to prevent any type of hacker access. When the router control connection is isolated from Ethernet ports with customer data it is termed an out-of-band management connection.

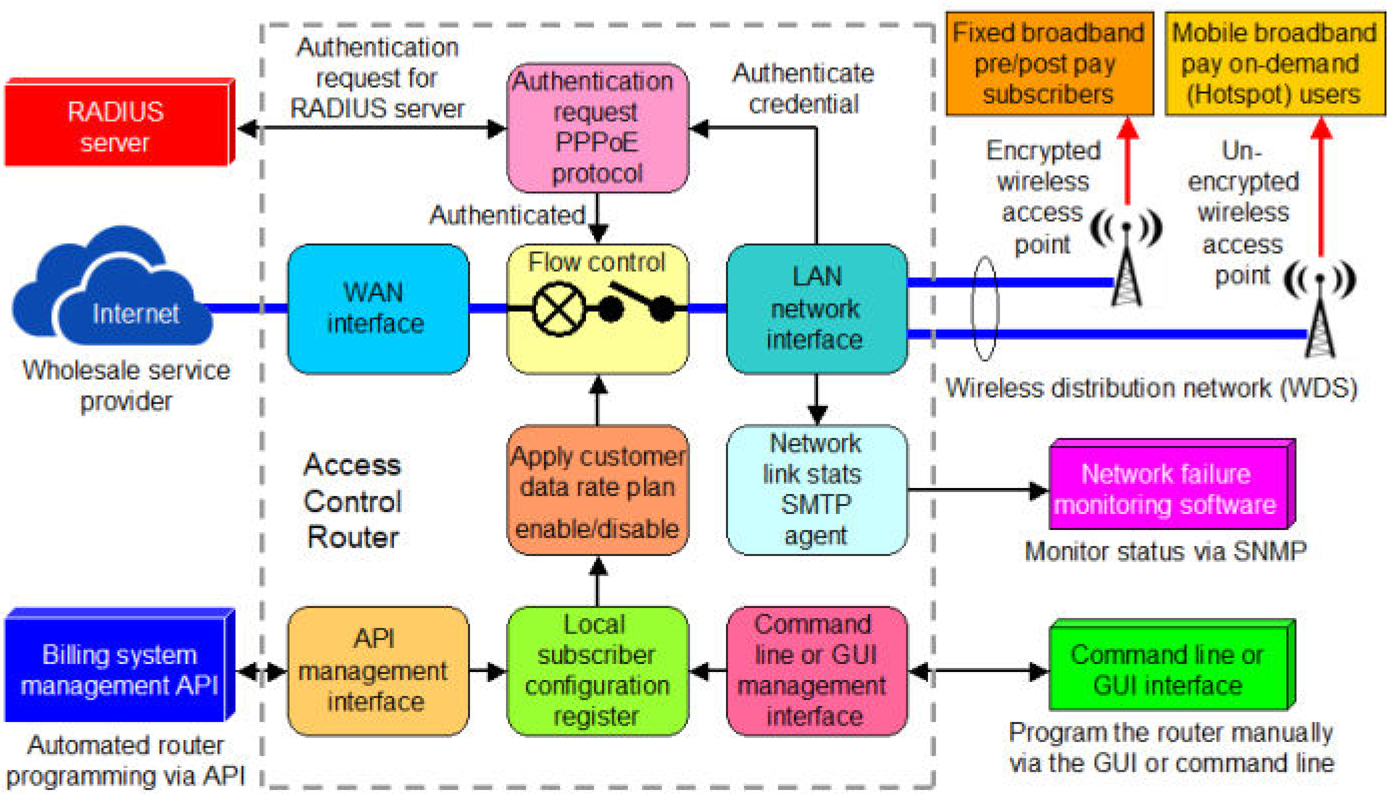


Figure 5.9.1. Process flow of the access control router programming.

The manual programming method requires significant study to become competent with the router programming language. Each type of router has a unique instruction set; for example the routers manufactured by Mikrotik have a software called RouterOS which has a specific instruction set. Routers can be programmed using command line instructions, and some routers have a graphic user interface (GUI), which simplifies the process of configuring the router, however the GUI does not have the flexibility and versatility of command line programming.

The WISP can choose to implement management software that will install an initial set of commands to program the router, and then control each customer access via commands to the router API.

The router programming implements a process flow logic that determines how the router manages each data packet that originates from customers connected to the network via the PtMP towers and the wireless distribution network. The router connects to a number of external devices, via router Ethernet ports; a router will have several Ethernet ports, usually from 5 to 10 ports.

The external interfaces to the router are listed below.

- One or more LAN ports that connect to the wireless distribution network or directly to PtMP wireless access points. This port receives incoming data packets from customers.
- A WAN port connects to the wholesale circuit provider for the Internet connection. This may be a single WAN port or can be two or more WAN ports, each connecting to a different wholesale provider for redundancy. The multiple WAN ports will be configured using router commands for load balance, which will aggregate the throughput of all wholesale circuits, and failover so that when a wholesale circuit fails the data traffic is redirected to other wholesale circuits.
- Network monitoring software periodically requests the router SNMP agent to provide information about router status and router traffic. If the SNMP agent does not respond then the network monitoring software will assume that the router or the circuit to the router has failed and send an alert to the network administrator.
- When a LAN port receives a data packet from a customer who is starting a new session the identity of the user has to be authenticated. Assuming that the network is designed to use the PPPoE protocol for customer communications over the network, then the customer CPE will send a pre-programmed credential to the router PPPoE server, which will request the external RADIUS server to authenticate that credential. If the credential is authenticated the PPPoE server enables the flow control for that session. Other authentication protocol methods can be implemented, such as WPA2-enterprise, which will use the RADIUS server.
- The router has both a command line and GUI interface that is used to configure the router and can be the method of managing the router with ongoing requests to add new customers to the network, and to deactivate non-paying customers.
- The API interface can be used by external software such as the billing system to add customers to the router access control table and to remove customers. Before the API can be used the router has to be configured using the command line or GUI interface. To simplify the configuration process the software provider

will give the WISP a script file that contains the command line instructions that are required by the software to start using the API. The WISP has to use the command line interface to load the script file into the router, which will enable the API. Subsequently the billing software manages the router access control process. The command line scripts are specific for each type of router, Mikrotik routers have a different set of commands to Cisco routers so the WISP who wants to implement a software to automate the access control process must verify the types of routers that the software provider supports.

The process flow begins with data packets that are received from a customer. When a new customer session is authenticated the customer has access to the Internet. If authentication fails then the customer has no Internet access. Rate plan rules are imposed on the customer by the flow control, which takes input from the subscriber configuration table that is programmed either manually or by the WISP management software. The rate plan will determine the maximum download and upload speeds for that customer, and also impose a data cap if that has been programmed. Internet access remains open for the customer providing that the bill is paid. If payment is not received then the customer is deactivated until the bill is paid.

Automated configurations for general-purpose routers require a constant input of information from the management software during operation. Some software manufacturers have developed routers with dedicated access control software that has much better throughput performance and greater functionality than that of a pre-programmed general-purpose router, including the RADIUS server functionality that is programmed by the management software. An important characteristic of the dedicated access control routers manufactured by software companies is that that they download part of the billing system database into the router and have the authentication database for the customers who will access that router. The dedicated router can therefore function autonomously without input from the management software until a new customer is added. This feature adds an additional layer of redundancy to the WISP operations and will ensure that customers continue to get Internet service even if the management software goes off-line.

5.10. Summary

The key points or take-a-way's that a WISP entrepreneur should remember when selecting the business administration software are listed below.

- The WISP's business processes should follow the software administrative model so that the WISP can make the greatest use of WISP management software.
- When developing service rate plans, it is important to get feedback from the potential customer base to discover what type of services prospective customers are willing to pay for.
- Initially the owner of a WISP start up business will fill all the roles required by the business. The WISP owner should take care when hiring people to ensure that the cash flow remains positive.

- Depending on the management software chosen, a smaller or greater part of the order entry, provisioning and activation processes will require manual methods using spreadsheets to log and track data.
- Customer billing is critical for the success of the business and requires constant monitoring and management to maintain the business cash flow.
- Network management and monitoring requires great care to maintain the reliability of the network, frequent failures will drive customers to other providers.
- Use the Customer Relationship Management (CRM) software to monitor the interaction with customers and solve any problem quickly to maintain customer satisfaction with the services provided.
- To implement manual management of access control routers a deep technical knowledge of programming routers is essential. Alternatively select administration software with an API interface to automate management of a popular brand of routers.

6. Planning a WISP business start-up

6.1. Considerations before starting a WISP business

Before beginning investments with a WISP business start-up, it is important to analyze the viability of the proposed WISP business. The analytical process to evaluate if a WISP business can make a profit and recover the initial investment is called a business plan. The plan however is an approximate estimate of the results that the business may or may not generate. When a new business is established it will usually perform differently to expectations and so the business owner must be prepared to adapt quickly to changing conditions, and possibly pivot to service different opportunities.

To prepare the business plan, evaluate the basic business parameters that will demonstrate if the business will be a success or failure.

- Estimate the charges that can be made for Internet services, with several rate plans that are researched to prospective customers.
- Estimate potential sales numbers based on what prospective subscribers can afford.
- Estimate the cost to generate sales, sales people, marketing, etc. then divide by the number of expected subscribers to be acquired, this is called the subscriber acquisition cost.
- Estimate the start-up costs required to begin providing the Internet service. This includes building the network infrastructure.
- Estimate the on-going operating costs of the business. This includes the service charge from the wholesale network provider.
- Calculate the expected income vs. costs. Is there a profit? if not then go back and increase the charge per subscriber. Will the price increase reduce the number of potential subscribers?
- Estimate the cost to scale the business, to expand the service for more subscribers and the cost of acquiring more subscribers.

Lets assume that the business opportunity will provide a wireless Internet service for the neighborhood of a small town. The questions to ask are:

- Is there already an Internet service provider, wireless or DSL, in the neighborhood?
- If so, how many people who want Internet access can afford to pay for the Internet service that is available?
- If not would there be a demand for a new Internet service, and if so what is the price that people are prepared to pay for the service?

- Do the people who want Internet access have a device that can access the Internet, a smart-phone, a tablet or a computer?

The prospective WISP owner must talk with people in the city neighborhood or rural area where the service will be offered. Use residence and business information available from the local government to discover how many homes and businesses are in the neighborhood. If there is an Internet provider estimate how many subscribers the current provider has to calculate a percentage of homes with Internet. If the answer is that very few people have the current service because it is expensive then there is probably a good opportunity to sell a lower cost wireless Internet service. It is possible to pick up subscribers who want to switch from an expensive service to a new lower cost service.

If people do not have devices that can access a wireless Internet service then an investment of an Internet café may be a better alternative. Products such as those manufactured by Guest Internet include a complete point of sale (PoS) for an Internet café.

People who have a smart-phone can get Internet access through their mobile service provider, however they will have a data cap, maximum number of data bytes per month with additional data requiring an extra payment. The data cap and additional charges may make a low cost wireless Internet service look attractive. In some parts of the world a mobile phone service is either not available or only available for calls.

The analysis must evaluate the ability of prospective subscribers to pay the estimated charge for the proposed WISP service. If potential subscribers cannot afford a DSL Internet service, then how much can they afford to pay for a wireless Internet service? If there is no Internet service available then how much are they willing to pay?

The WISP can adjust the services for potential subscribers who have different economic situations by offering a multi-tier service with several rate-plans; an example of four rate-plans is listed below;

- Maximum 5Mb/s download speed; 500Kb/s upload speed; $10/month.
- Maximum 10Mb/s download speed; 1Mb/s upload speed; $18/month.
- Maximum 25Mb/s download speed; 2.5Mb/s upload speed; $40/month.
- Maximum 50Mb/s download speed; 5Mb/s upload speed; $75/month.

As the speed gets higher the WISP can offer a cost saving incentive to persuade prospective subscribers to move up to the next tier. The prices listed above are high for developing economies where people have limited money to spend. In developing economies additional lower-cost tiers can be added, such as the examples below.

- Maximum 1Mb/s download speed, 100Kb/s upload speed; $2/month.
- Maximum 2.5Mb/s download speed, 250Kb/s upload speed; $5/month.

A maximum download speed of 1Mb/s might sound very low compared to what subscribers are accustomed to get in industrialized countries, however it is adequate for email and social media services; it is slow however for video streaming services.

Considering that the parents of today's young generation started their Internet access experiences with a dial-up modem at 56Kb/s or less, 1Mb/s is quite fast.

Finally consider the cost of providing the service. The range of a PtMP wireless access point antenna that will provide the Internet service for the neighborhood is limited and so the potential subscribers per wireless will be limited to a radius around the antenna tower site. In the case where the research is conducted over a large area, an estimate must be made of how many wireless access points and antenna towers are required to cover the area. More wireless access points will also increase the cost of the equipment required to provide access for the estimated number of potential subscribers. The ideal plan is to start small, with one wireless antenna tower site and one Internet trunk connection. Sell the service to people who are within range of the antenna until the maximum capacity of the Internet backhaul and wholesale circuit is reached. Then plan to expand to a second antenna site and increase the Internet wholesale circuit capacity.

6.2. Estimate subscriber sales volume and income based on charge per subscriber

Document how many potential subscribers there might be for a WISP service and how much each potential subscriber is willing to pay for that service. For example, if 20 potential subscribers are willing to pay $10 per month for a service of 10Mb/s then that equates to $200 per month potential income for a 200Mb/s circuit. If 100 potential subscribers are willing to pay $5 per month for a basic service of 2Mb/s then that equates to $500 per month of potential income for a 200Mb/s circuit.

The contention ratio (the degree to which the capacity of the backhaul will be oversold) multiplies the number of subscribers that can be connected to a service. In the first example with a contention ratio of 2:1 then 20 subscribers each with a maximum of 10Mb/s connection can be connected to a 100Mb/s backhaul circuit. In the second case where more subscribers are connected at a slower speed the value of the contention ratio can be increased to 4:1. Therefore 100 subscribers with a 2Mb/s service can connect to a 50Mb/s backhaul. The WISP will have to experiment with the contention ratio value to ensure that subscribers receive an adequate service.

Calculate the cost of the Internet backhaul circuit for the number of estimated subscribers, based on the chosen contention ratio.

Potential subscribers might be outside the range of one PtMP wireless antenna or not have line-of-sight (LoS) and so multiple wireless antennas might be required to cover the area where the potential subscribers are located, which is an additional investment cost for the WISP.

After speaking with prospective subscribers a conclusion can be made about the charge that people are willing to pay and how many people might become subscribers to get an estimate for the potential income of the proposed WISP business. This potential income will be offset against the cost of operating the business. This potential income from subscribers and operating costs will be used to estimate the profit or loss of the proposed business.

6.3. Start-up costs

The start-up cost covers all equipment and services that are required to provide the Internet service to subscribers. A PtMP wireless access point with antenna will be required, and several wireless access points will be required to cover a large area. There will be a monthly rental cost for the location of the wireless access point antenna, either on an existing tower or on the roof of a building. There also may be antenna installation costs if the WISP owner is not able to install the antenna on an existing tower, or if the WISP has to purchase and install a tower. It will be necessary to pay contractors for the installation.

The ISP providing the wholesale Internet trunk connection may charge fees to initiate the service. If for example an ISP is contracted to provide a circuit at a building where the antenna is installed, then an installation fee will be charged, and the ISP may charge for the modem or router. It will also be necessary to purchase and install an Ethernet cable that connects the ISP router to the top of the tower or roof of the building.

It may not be possible to have the Internet circuit installed in the building or tower where the antenna is installed. In this case an additional point-to-point wireless link will be required to connect the location where the antenna is installed to the network operations center location where the ISP circuit is available.

The WISP requires a method of billing subscribers for the service; there will be a purchase or lease cost for software or a cloud service cost. Software will be purchased for network monitoring. The advantage of contracting with a cloud management service is that there is no initial investment cost, only a monthly operating expense. Another initial expense is the equipment required to build the wireless distribution network, that includes switches and routers, and the router required for the access control function.

6.4. On-going operating costs

The wholesale trunk circuit from the WISP NOC to the Internet Service Provider backbone is a significant operating cost. This might be a copper or fiber connection, or a wireless point-to-point (PtP) link to the ISP's point-of-presence (PoP). There will be an installation charge in addition to the monthly charge. In some parts of the world the ISP may also charge per Gbyte of data downloaded. Before signing a long-term agreement, verify that the ISP permits the Internet service to be resold. Some ISP's may require the WISP to pay for a more expensive service for resale to customers. In many cases the ISP will not be concerned with how its customers are reselling the service.

It may be necessary to have several antenna sites in order to provide Internet access for the desired area of coverage. The WISP may have to choose between installing an ISP service at each antenna site, or installing a faster ISP service at the central NOC site, then distributing the service to other sites using wireless point-to point-links. This is a technical decision determined by cost vs. performance.

6.5. Cost to generate sales

There will be several costs to generate sales. Although generally managed as an operational cost, customer acquisition is actually an investment cost. The most important cost item is marketing. Prospective subscribers will only know about the wireless Internet service if they are informed about it. There are many methods of advertising the service to prospective subscribers. For a small neighborhood, the best marketing solution might be to print flyers and then go door-to-door posting the flyers; this may take a few days but will ensure that all residents in the neighborhood are aware of the service. Of course the flyer must explain the advantages of the service, especially the low cost, and the easy installation. Provide a contact telephone for people who want to ask questions and who want to sign up for the service. Distribution of flyers can be repeated periodically after the business has begun operations. Limited time introductory offers are always an incentive to initiate sales. A WISP who wishes to cover a large geographic area can advertise in a local newspaper, or other communications channels that have access to the potential subscribers.

Create a website for prospective subscribers who want to read more via their smart-phone provider and provide an email address so that prospects can send a message to request information about the service.

6.6. Profit or loss and investment amortization

The estimate for profit or loss will be approximate, but will give an indication about proposed WISP business being viable. It is likely that business plans will change when the business is operational and the WISP discovers where the real demand for services is located, or subscribers wish to pay for a service that is different to those that the WISP was planning to offer. A start up business should always be very flexible and be ready to pivot in a different direction as feedback is received from prospective customers.

The profit/loss calculation is actually an on-going process that is adjusted and updated with each change in the business direction. Very soon the WISP owner will carry the profit/loss calculation in his/her head and be able to make quick decisions about business changes.

Prepare a profit or loss table like the one shown next for the estimated monthly income and monthly costs. Determine if the estimates show that the business will generate a profit or loss.

The estimate for the profit or loss statement will indicate if the WISP start-up is a good business idea. If the business idea does not appear to be good then look at alternatives, maybe an Internet café will be a better investment?

If the business can generate a profit, calculate the time taken to amortize (recover) the initial investment. This is the time taken for the amount of profit obtained to equal the amount of money that was invested to start the business. The table shows how the amortization is calculated.

The business might be profitable but if the initial investment is so large that the amortization takes several years then starting the WISP business may not be a good plan. Most WISPs' make the minimum possible investment to start the business and begin receiving income. The WISP will then allocate a percentage of monthly profits towards building out the network to support more subscribers while the sales staff is attracting new subscribers in parallel.

Item	Cost	Income
Potential sales		$ Estimate of monthly sales
Cost to generate sales	$ Monthly marketing cost	
On-going operating costs	$ Monthly DSL and tower rental	
Cost to scale	$ Monthly equipment investment	
TOTAL	$	$
Profit or loss?	($ Total income) – ($ total cost) = +$ (profit) or -$ (loss)	

Table 6.6.1. Estimating profit or loss.

Item	Investment Cost	Monthly Net Profit
Cost and profit	$ Equipment/labor investment	$
Amortization time?	($ Equipment investment) / ($ profit) = months to recover the investment	

Table 6.6.2. Estimating return on investment.

6.7. Scaling the business size

WISP owners are constantly looking to expand the network and acquire more customers. As the size of the business increases with more customers then the operating cost per customer will fall, increasing profitability. The cost reduction occurs for several reasons.

- Network infrastructure has a minimum fixed cost, and when more customers are sharing the resource then the cost per customer is reduced.

- A wholesale circuit cost per Mbit of bandwidth will reduce as the capacity of the circuit increases, a 1Gbit/second circuit will cost less per Mbit of bandwidth than a 100Mb/s circuit.

There are two primary investment costs that are incurred when scaling up the business operations to add new subscribers.

The first cost is due to increasing the data capacity of the infrastructure. Adding wireless access point antennas and towers are necessary to cover a larger or different geographic area. This will enable the Internet service to be provided for more potential subscribers. As more customers are acquired it will be necessary to install more PtMP wireless access points at the tower location as one wireless access point has a limited capacity, which may be approximately in the range of 50 maximum subscribers for a low cost wireless access point to 300 subscribers for a high performance dual band wireless access point. A wireless access point does not have a connection limit, however it does have a performance limit that will determine the maximum number of subscribers that can be connected before the service begins to deteriorate. A second antenna at the same location will allow the connection of additional subscribers however the backhaul connection to the ISP will require an increase of bandwidth. Each adjacent antenna should be set to a different non-overlapping frequency. The cost of Internet trunk circuits will increase as the WISP increases the backhaul capacity.

The second cost is that of customer acquisition. When the WISP business is established the cost to acquire new subscribers will be estimated; divide the money spent on sales people and marketing costs by the number of subscribers obtained. Customer acquisition cost will scale up however as the area of coverage is increased, more sales and installation staff will be hired who will have to travel greater distances to visit customers, adding to expenses.

6.8. Decisions about how the business will operate

There are two important decisions about cost and income that must be made when planning the business startup; these are installation charges and monthly service charges.

The first decision is regarding the addition of new subscribers to the network. In order to provide the service there will be a cost to connect that subscriber due to the installation of wireless CPE and network equipment at the subscriber’s premises, residence or business. The WISP owner must decide how to manage this cost. If the WISP decides to charge an installation fee then the prospective customer may not be able to afford the fee and so the WISP will loose a potential subscriber. Alternatively the WISP does not charge the subscriber an installation fee but expects to recover the installation cost over several months by adding a charge to the monthly bill to cover the installation service and equipment cost. Amortization of the cost is an acceptable solution only if the WISP has a financial reserve to cover the installation cost, and the WISP can rely upon the subscriber to continue paying monthly fees during a contractual period, which might be one year, so that the WISP can fully amortize the cost of the installation. Whatever the decision the WISP makes, it will be necessary to draft a contract for the subscriber and the terms of such a contract will depend upon the laws of the location, country of state, where the WISP business is located. The WISP owner must ask a lawyer who is familiar with the laws that determine service provisioning for help to draft a subscriber agreement.

The second decision that the WISP must make is regarding the subscriber rate plans and billing rates. The WISP has two major fixed operating costs for each PtMP tower location. These costs are listed below.

- The cost to provide broadband access for the antenna tower; the WISP will pay a monthly fee to an ISP.
- The cost of locating the PtMP antennas on the tower or building, this will be a rental fee for the space used, probably a charge per antenna.

The WISP has to divide these charges between the subscribers that are connecting to the tower, and add to this number other fixed costs of the business. Some of the other fixed costs are listed below.

- Payroll and overheads for the cost of staff.
- Rental for the premises where the NOC is installed.
- Power for the NOC and other sites.
- Rental for locations where PtP antenna relay-repeaters have to be installed between the PtMP antenna tower and the NOC.
- Equipment purchases for the maintenance of the network.

The WISP therefore has to calculate a charge per Mb/s of data that the tower PtMP antenna is capable of providing, while factoring in the contention ratio. The WISP will have to determine where the break-even point will be for the tower. The number of subscriber payments at what rate plans that will be required monthly to pay the operating cost of the tower determines the break-even point for a tower. Operating at break-even does not generate profit and so the initial investment cannot be recovered. However the operating cost of the tower will be paid. It is very important for the WISP to ensure that the minimum number of customers quickly become subscribers as soon as the tower can provide service for customers. This will require the sales staff to pre-sell Internet access to ensure that the customers are available when the tower becomes operational.

With capacity below the break even point the WISP will loose money, with the capacity above the break even point the WISP will make a profit. As an example, calculate the break-even point at 40% of the tower capacity.

- ISP backhaul circuit cost per month: for a 50Mb/s circuit: $100/month.
- Tower charge per month for the antenna space rental: $50/month.
- Add other overheads that the WISP has for operating the business, divided by the number of towers: $30/month.

Total cost to provide up to 50Mb/s of bandwidth is 100+50+30 = $180/month.

- Assume the contention ratio is 5:1, the WISP can sell up to 250Mb/s of bandwidth for that tower.
- Choosing the tower break even at 40% means that the sale of 250x0.4 = 100Mb/s of bandwidth will pay the cost of the tower.
- Calculate the charge per Mb/s of bandwidth: 180/100 = $1.80 per Mbit/s of bandwidth.

This means that if the WISP sells a subscriber a maximum download speed of 10Mb/s then the WISP must charge that subscriber 10x1.8 = $18 per month. This determines the rate-plan parameters.

In order to break even the WISP must sell ten of the 10Mb/s plans to subscribers. The WISP can sell up to 25 subscribers plans of 10Mb/s and so the 11th and upward subscriber will represent a profit for the WISP. With 25 subscribers of 10Mb/s each the tower will generate 15x$18 = $270/month gross profit. Net profit will be less as part of the profit will be used to expand the network so that more customers can be added, and part of the profit will be used to amortize the initial investment.

Some subscribers will have a limited budget and seek a lower cost service, whereas some subscriber's can afford to pay for a fast service. The WISP must therefore elaborate rate plans that will suit a wide range of financial abilities. Rate plans offered by the WISP might look like the following list when charging the service at $1.80 per Mb/s of bandwidth.

- 5Mb/s for $9/month.
- 10Mb/s for $18/month.
- 25Mb/s for $45/month.
- 50Mb/s for $90 per month.

The values listed above can be modified to encourage a subscriber to move up to the next tier to get a lower charge per Mb/s of data. A revised table might look like the following:

- 5Mb/s for $11/month = a charge of $2.20 per Mb/s.
- 10Mb/s for $20/month = a charge of $2.00 per Mb/s.
- 25Mb/s for $48/month = a charge of $1.92 per Mb/s.
- 50Mb/s for $90 per month = a charge of $1.80 per Mb/s.

Note however that fewer high bandwidth customers will require the contention ratio to be reduced and so moving a customer to a higher data rate might be counter-productive. The WISP has to make this calculation for each subscriber mix.

The break-even point regarding the number of subscribers will change with multiple rate-plans. If all subscribers choose the lower cost plan then more subscribers are required to achieve break-even, however the contention ratio can be increased. If all subscribers choose the higher performance plan then less subscribers are required to achieve break-even but the contention ratio must be lowered.

The cost of subscriber acquisition stays fairly constant for different types of subscribers, those who want to pay low fees, vs. the subscribers who want high performance. Fewer high performance subscribers will cost less to acquire than more low cost subscribers, however the contention ratio will be lower for high performance subscribers as each customer represents a larger proportion of the total circuit bandwidth, so the income per backhaul circuit will be lower.

Subscriber acquisition includes the cost of sales people, advertising, retail space, etc per month, divided by the number of subscribers per month that the WISP acquires. As an example, assume the cost of subscriber acquisition is $100 per subscriber.

In a situation where the WISP has only economical subscribers purchasing the 5Mb/s service at $11/month then the maximum number of subscribers that the tower can support will be: 250/5 = 50 subscribers. The WISP will have to pay the acquisition cost of 50x100 = $5,000 to acquire 50 subscribers. The income generated by the 50 subscribers will be 50x11 = $550/month. As the fixed cost is $180 per month then 16.3 subscribers will be required to reach break-even, and 33.7 subscribers will generate a profit of $370.80/month.

In another situation where the WISP has only high performance subscribers purchasing the 50Mb/s service at $90/month the maximum number of subscribers that the tower can support will be: 250/50 = 5 subscribers. The WISP will have to pay the acquisition cost of 5x100 = $500 to acquire 5 subscribers. The income generated by the 5 subscribers will be 5x75 = $375/month. As the fixed cost is $180 per month then 2.4 subscribers will be required to reach break-even and 2.6 subscribers will generate a profit of $234.

In practice the subscribers will be a mix of economical and performance subscribers, with subscribers located between the two extremes. There is a tradeoff between the numbers of desired subscribers vs. the cost of acquiring a subscriber.

It is clear that the WISP has several parameters that must be juggled to optimize the profitability of the business, and each scenario will have a different calculation with different priorities.

The WISP should repeat the calculations described above in order to determine how the services should be priced for the subscribers to ensure that the WISP does not loose money. The situation can be complicated further if there is a competitor in the same market which will require that the startup WISP has to charge lower prices than the competitor. The competitor might be a wire-line ISP offering a DSL service and the startup WISP must offer lower prices in order to attract subscribers from the service that they currently use. There is also another factor. When a subscriber has been with an ISP a long time and the service is good then the subscriber is resistant to change even when a competitor offers lower prices. In fact ISPs feel comfortable to increase subscriber charges annually with the expectation that the subscriber will be resistant to change to a lower cost provider.

6.9. Investment and operating cost examples

The tables that follow provide additional information for new WISPs about the typical start-up investment and on-going operating costs.

Investment item	Investment description	Approximate cost
Tower PtMP.	PtMP wireless access point for installation at the tower.	Multiply by the number of towers.
Tower PtP.	PtP wireless for backhaul to the NOC if the tower has no Internet access.	Multiply by the number of towers.
Tower power.	If no power with backup is available at the tower a solar and wind generator with battery backup to power equipment is required.	
NOC wholesale connection.	Service charge to install the wholesale Internet connection at the NOC.	
NOC Power.	Backup generator to power the NOC in the event of power failure.	
NOC power install.	Electrical services to rewire the NOC so that a backup power can switch over in the event of a power failure.	
NOC computers for management.	Purchase of computers to run management software.	
NOC central router for access control.	Central router installed at the NOC with the capacity for all traffic.	
NOC tower router for access control.	Where the tower has Internet access, install a router for access control at the tower with capacity for all customer traffic at that tower and manage the router remotely.	
NOC Ethernet switches.	Ethernet switches are required together with patch cables to interconnect all equipment at the NOC.	
NOC antenna tower (optional).	It might be possible to install PtP antennas on the roof of the NOC, otherwise purchase and install an antenna tower close to the NOC for the PtP antennas.	
NOC wireless PtP links.	A PtP wireless unit for each link to a PtMP antenna tower.	
NOC A/C.	NOC air conditioning to keep equipment and staff cool.	
NOC tower installation.	Services to install PtP antennas on the tower at the NOC site.	

Tower installation.	Services to install antennas and equipment on a tower (in the USA a licensed and insured tower climber must do the installation work.	Multiply by the number of towers.
PtMP tower purchase.	If no tower is available then purchase one.	Multiply by the number of towers.
PtMP tower installation.	If no tower is available then pay to install a purchased tower.	Multiply by the number of towers.
Management software purchase.	Software purchase is an alternative to leasing software or paying for the service of a cloud provider.	
Vehicle purchase.	One or more trucks must be purchased or leased for the field service technicians to install equipment at the customer premises and for tower maintenance.	
Tools.	Installation tools for the field service technicians.	
Customer site installations parts.	Maintain an inventory of customer premise installation kits, CPE wireless, outdoor Ethernet cable, PoE supplies, wireless routers, Ethernet patch cords.	
Bookkeeping software.	Purchase or lease of bookkeeping software to maintain ledger, accounts payable and receivable and payroll.	
Fire equipment.	Installation of a fire alarm and extinguishers at the NOC to meet legal requirements.	
Tower and PtP repair parts inventory.	Maintain an inventory of parts to repair tower installation and PtP links that are damaged by lightening strikes or hurricanes.	

Table 6.9.1. Typical start-up investment costs for a WISP.

Operating cost item	Operating cost description	Approximate cost
Tower PtMP antenna space rental.	Monthly charge for a PtMP antenna installed on a tower.	Multiply by the number of towers.
Tower PtP antenna space rental.	Monthly charge for a PtP tower antenna that provides a backhaul wireless connection to the NOC, for the case where the tower has no Internet access.	Multiply by the number of towers.
Tower service utilities.	Monthly charge for electrical power and Internet to the tower if available.	Multiply by the number of towers.
NOC building rent.	Monthly cost of rent for the NOC building.	

Tower ground rent.	If there was no PtMP tower and a tower was purchased and installed then there is a monthly ground rent for the installation site.	Multiply by the number of towers.
Admin cloud service.	Monthly charge for the cloud services required to administrate the subscribers and network.	
Staff salaries.	Payroll will be a significant cost overhead.	
Utilities at the NOC site.	Electrical and water utilities.	Multiply by the number of towers.
Wholesale Internet provider.	Monthly charge for the wholesale Internet connection to the NOC.	
Marketing.	Monthly marketing cost to attract customers.	
Financial charges.	Cost of transaction processing systems, credit cards, debit methods, cash payment methods.	
Retail store.	Optional retail store for the WISP to sell agreements, demonstrate the service and receive monthly payments from customers.	
NOC backup power.	Monthly cost of operation, gasoline, etc as the equipment must be tested every month.	
Insurance.	Liability insurance, workers compensation, etc., which are legal requirements.	
Customer premise installations.	Monthly cost of installing CPE equipment at customers premises.	
Training.	Periodic training courses for staff, technical, administrative.	
Maintenance.	Maintenance services for the NOC building, property taxes, etc.	

Table 6.9.2. Typical on-going operating costs for a WISP.

6.10. Preparing a WISP business plan

Many people start a business without a business plan and later find that lack of proper planning caused a failure of the business or that the business had to pivot several times to become profitable. It is very important to have a detailed plan in place before spending with the initial investment. The business plan has a series of advantages.

- Thoroughly understand the market opportunity, including the type of service that potential customers are seeking (the rate plans).
- Through research with potential customers calculate an accurate estimate for the potential income based on the rate-plans that people can afford and the potential number of subscribers.
- Prepare a marketing plan that will inform all potential customers about the service to be offered and the advantages when compared with similar services.
- Prepare a detailed financial plan for the investment required to provide a service for potential customers with an investment timeline.
- Prepare a detailed financial plan for on-going operating expenses to deliver the service to the prospective customers.
- Prepare a pro forma (estimated) cash flow plan based on operating costs with expected income from customers.
- Estimate the time to break even for operational expenditure vs. income.
- Prepare a pro forma (estimated) profit or loss (P&L) statement for the first year of operation based on the estimated cash flow.
- Estimate the time taken to recover the initial investment (ROI) based on the net margin generated by the estimated cash flow.

The entrepreneur should evaluate the possible success or failure of the business based on the analyses listed above. If the business results are weak then the entrepreneur must adjust the plans to identify how the business results can be improved.

- How can the number of prospective customers be increased?
- How can the income per customer be increased?
- How can the initial investment costs be reduced?
- How can the operating costs be reduced?

In addition a business plan will be requested whenever the entrepreneur seeks financial or business help.

- When procuring a bank loan.
- When seeking an investment partner.

A business plan can be prepared in a number of different formats, however two factors must be elaborated in detail.

- The description of the business and the results expected must be clear and concise.
- The plan must include all information that lenders and investors are seeking.

6.11. Business plan contents

A suggested list is presented below for the business plan contents.

- **Executive summary**: A single paragraph that will explain what the business will do and the results that the business will achieve. Prospective business partners, bank managers and investors are busy people and will not have the patience to read the whole plan to understand the business and what is expected from it.
- **Description of the business**: avoid using technical language and write for a non-technical reader.
- **Mission and vision statements**: Write a short sentence for each statement. A mission statement focuses on the present and what an organization is doing to achieve its goals. A vision statement focuses on the future and what an organization will ultimately become. The statements direct the immediate and long-term goals for employees and tell customers what the business is doing and where it is going.
- **Industry overview**: What are the products or services? What are the market demographics? Who is currently delivering the products and services and to whom? What are the various methods that the products and services can be delivered? What are the limitations of the industry? What is the demographic that currently has no access to the products and services proposed by the business?
- **The market opportunity**: Who are the customers of the new business? Where are the customers? What service do the customers want? How much are the customers prepared to pay? How many customers are there? Do competitors provide similar services? If there are competitors what are their services and what do they charge?
- **What and how will the business deliver**: Describe each service in detail and how each service fits each market opportunity, determine the rate-plans and on-demand plans where each plan should be justified by basing it on market research. Describe how each service will be provided for the customer and the infrastructure required for providing the service. Describe and identify the suppliers that will be required by the business so that it can provide the service to the customers. Describe the regulatory steps that the business requires to operate, including insurance, permits, and licenses. Describe the properties that the business requires to operate, offices, NOC, tower sites and relay sites. Describe the installation at the customer's premises so that the customer can receive the services.
- **Sales and Marketing**: How are the potential customers going to be informed about the service through publicity and marketing? What is the process for customers to obtain the service through sales? How will the service be delivered to the customers through installation? How will the customers be charged for the service? What will happen if there is a failure with the service delivery? What will happen if the customer fails to pay for the service?

- **SWOT analysis**: What are the **strengths** of the business? What are the **weaknesses** of the business? What are the **opportunities** for the business? What are the **threats** to the business?
- **Business organization**: describe the areas of activity of the business departments, and the requirements and deliverables of each. What are the staffing requirements of each department? What is the staffing proposal as the business grows?
- **Roles and responsibilities**: Who are the business founders and what are their biographies? What are the shareholders participations in the business? Do the founders have business start-up experience? What are the staff roles in the business and include a job description for each? What are the qualifications required for the staff roles?
- **Startup investment**: What will the cost be for the business to become operational and begin delivering services to customers? Provide a spreadsheet to document startup costs.
- **Source of the startup investment**: Will the entrepreneur provide the business funding? Does the entrepreneur have an investment partner? Will the entrepreneur require secured loans? How will the investment be provided, initial sum or as stage payments? Will the entrepreneur have access to additional investments to support the business until it reaches break-even?
- **Monthly operating costs**: Prepare a plan of monthly operating expenditures to deliver the services to customers and include purchasing customer CPE kits, and sales and marketing costs. Provide a spreadsheet to document operating costs.
- **Expected monthly reinvestment costs**: A monthly budget will be required for infrastructure maintenance and repairs, and infrastructure expansion to permit adding customers. Infrastructure expansion includes, adding PtMP towers, expanding NOC capacity, and increasing the ISP backhaul capacity. This budget may also include adding new towers with LEO satellite backhauls, and switching some existing towers to LEO satellites when the service becomes available. Provide a spreadsheet to document reinvestment charges.
- **Expected monthly income**: How many customer sales are expected each month? What is the expected income per customer? What are the expected monthly sales? What is the expected monthly income? What is the expected month over month income growth? Provide a spreadsheet to document expected sales income.
- **Month by month cash flow for the first 12 months**: Subtract monthly operating costs and monthly reinvestment costs from expected monthly income for each month showing monthly positive or negative revenue. Provide a spreadsheet to document cash flow over the first 12 month of operation. It may be necessary to prepare spreadsheets for 13 to 24 months and 25 to 36 months for the subsequent ROI calculation.

- **Milestones**: Set points along the cash flow timeline for achievement goals, the goals may be the number of subscribers connected by a certain date, or a numerical sales figure. Encourage staff to achieve the goals, possibly by giving rewards, to ensure the expected business performance parameters are met.
- **Identify the break-even point**: This is the date on the cash flow timeline where the cash flow revenue becomes positive. Minimizing this time duration is critical and the entrepreneur should pre-sell the service so that the business has a number of customers initially to shorten the time to break even.
- **Calculate the operational investment required**: Calculate how much additional investment is required to support the business over the period that the cash flow revenue is negative.
- **Calculate the time to obtain a return on the investment (ROI)**: This is calculated by adding the startup investment to the operating investment over the negative cash flow period. Calculate the ongoing revenue after cash flow is positive and determine the time taken to recover the startup plus operating investments.
- **Future business growth**: After the ROI period the business will generate a profit however ROI may take more then one year. When the ROI is completed the entrepreneur can consider increasing monthly reinvestment costs using profits to speed the growth of the business. Include a plan to show how the business can grow over a 3 to 5 year period based on the demographic of the customer base.
- **Exit strategy**: Does the entrepreneur expect to grow the business indefinitely without any plan for sale or merger? Does the entrepreneur have a plan to exit the business through a sale or acquisition partnership? After what milestones can the business expect to be sold or merged? What is the expected sale price or merger value based on similar business activities?

An important use of the business plan is a tool to compare expected results with reality. When the business is operational update the spreadsheets each month with investment, expenses and sales data in order to track the actual business results compared with the expected results. If the actual results deviate considerably from the expected results and the results do not meet cash flow expectations then it will be necessary to pivot the business in a direction that will improve the financial performance. Changes may include offering different services to different demographics. Such changes may delay the break-even and ROI points.

6.12. Other business issues

The start-up WISP has additional issues that will add to the operating costs, which are listed below.

- Government regulatory issues.

Each country has regulations imposed on WISP’s by the government department that regulates telecommunications. The WISP owner must check with the government department about the legal requirements to start and operate a WISP business. WISP's located in the USA are required to collect a telecommunication tax from customers and pay this tax to the government. In addition WISP's are required to file a form 477 with the FCC twice every year. The FCC uses the information collected with this form to determine which WISP's service which areas and this information is used for planning purposes. The form is completed on line and PDF instructions can be downloaded from the FCC website.

https://transition.fcc.gov/form477/477screenshots.pdf

In some countries a WISP will need a government license to operate which will have a cost. There are countries that have a government telecommunications monopoly and it is illegal for anyone to start a WISP business. Needless to say such countries have very expensive telecommunications services using older technologies and are probably blocking access to Internet services to prevent the dissemination of information between users.

- Construction permitting issues.

Depending on the WISP's location and the municipal, state and federal rules regarding business installations, the WISP will likely need permits for installation work. A NOC site will require the service of a licensed and insured electrician who is qualified to request high voltage permits for power wiring, and low voltage permits for data wiring. Construction of an antenna tower will require a lot of permits, there will be several construction permits that include the foundation, and tower construction. It will be necessary for a civil engineer and mechanical engineer (both licensed and insured) to submit assessments regarding the strength of the construction. Environmental impact permits may be required and permits to install antennas on the tower, which will require a licensed and insured tower climber to install the antennas. In addition permits will be required for the construction at the base of the tower where the equipment is installed, and permits will also be required for the electrical and data connections to the equipment housing. It is usual that rural installations will require fewer permits than urban installations. There are locations in the world where none of this is needed.

- Organic growth vs. growth with loans or investments.

Organic growth is the business growth that is funded out of the business profits. There is a limit to the business profits so the rate of growth is limited by the business profits available. If the WISP wants to grow faster then the WISP has two alternatives, take out loans or bring investors into the business to provide capital. Each has a trade off. Any bank providing a loan will require collateral for the loan, if the WISP has no assets such as property then it may be difficult to obtain a loan. If the WISP owner brings an investor into the company then the investor will provide capital for investment, however the WISP owner no longer has sole control of the company, now the company management and profits are shared with the investor.

- Qualifying for loans.

Assuming that the WISP owner has collateral to support a loan, the lending entity will want to study the business information provided by the WISP. The WISP owner should be prepared to provide the business plan, a profit and loss statement, a statement of investment amortization and a revenue projection. The lending entity will want to verify that the business can afford to make the loan payments.

- Delegating responsibilities.

An entrepreneur will start a small WISP business and assume the whole workload to make the business operational. Initially the WISP owner does every task that the business operations require. As the business grows the workload becomes too great for one person and so the WISP owner has to make decisions about delegating responsibility to others. The WISP owner must decide which business processes are critical to the business operations and which business processes are not critical. Begin by delegating the non-critical business processes to staff in order to build trust with the member of staff. Some critical processes can be delegated when the WISP owner has a degree of trust in staff.

- Wholesale network service providers.

The WISP seeks to lease high bandwidth circuits for an economical cost in order to resell that capacity to many users. Wholesale network services are frequently available in urban areas, but less frequently available in rural areas. The WISP can only provide a service to customers when the WISP is within a few tens of Km from the wholesale data connection. In many countries rural areas have no wholesale circuit provider and the only circuit that the WISP might have available is a DSL connection from the telecom company. Frequently there is no type of Internet connection and therefore no WISP service. Some rural WISP's in Latin America and Canada use the Hughes satellite service as the Internet backhaul but the service is very expensive with very low bandwidth and is not very suitable as an Internet backhaul circuit. It is not the intention of Hughes to provide a backhaul circuit for WISP’s but to provide an Internet service for individual customers. The soon to arrive LEO (low earth orbit) satellite services are suitable for WISP's however with ten times the speed of the Hughes link and one tenth of the latency, for approximately the same cost as Hughes.

6.13. Summary

The key points or take-a-way's that a WISP entrepreneur should remember when planning a WISP Business start-up are listed below.

- Before starting a WISP business do the research to understand what will be needed and prepare a business plan.
- Knowledge of the market is essential to determine what rate-plan service products that can be offered to prospective customers. Estimate subscriber sales volume and income based on an estimated average charge per subscriber.
- When evaluating start-up costs do the research to find the minimum investment required to begin offering the Internet service to subscribers.
- When evaluating on-going operating costs the three significant costs are; operation of the NOC, monthly charge for the wholesale Internet circuit, and antenna tower rental space for the PtMP wireless and PtP backhaul.

- Estimate the cost to generate sales; this is the cost of marketing the service to create awareness with the target customer base and the cost of making a subscriber agreement with customers, which may require sales and customer support staff. Calculate the customer acquisition cost, which is the cost of attracting a subscriber, and is a business investment.
- Prepare an estimate for profit or loss and investment amortization as part of the business plan and update these numbers with each month of operations to track the performance of the business. This is also required to obtain loans or attract investors.
- The advantage of driving growth to scale up the business size is that a bigger business volume can reduce the operating cost per customer however it is necessary to delegate responsibilities starting with non-critical responsibilities first.
- Prioritize business investments to maintain good customer relations; happy customers will sell the service to others.
- Plan investments carefully to expand and grow the WISP business and get the most “bang for the buck”, that is the biggest income from the smallest investment.

7. Additional and third party services

7.1. Opportunities for a WISP to increase revenue per customer

Once a WISP has converted a prospective customer to a subscriber who is connected to the Internet then that is only the start of the relationship with that customer, not the end. As most readers will be aware big telecom companies offer at least three services. When a customer signs an agreement for an Internet connection then that customer starts receiving marketing and special offers for a phone service and a streaming TV service. The telecom companies will offer a discount to 'bundle' all three services. Some telecom companies also offer other services such as home security. Marketing additional services to existing customers is called up selling, and the cost of up selling is much less than the cost to acquire a new customer.

WISP's can also offer services like phone, TV plus a range of other services. The WISP does not have to develop the additional services as many companies have already done the technical work and so the WISP can become a reseller of these third party services. The services are "white-label" which means that they do not have a branding. The WISP can add the business branding and so the customer will understand that these services are created and provided by the WISP.

The WISP customer can also look for services that are available via the Internet and require the customer to pay a monthly subscription. Apple TV, Amazon TV, Netflix and Youtube are the most popular Internet TV services. A Voice over IP (VoIP) phone service is available from many companies. A Skype subscription will install a phone number in Skype so any computer or tablet can become a phone to make calls anywhere in the world. Some companies will sell an IP phone handset with a telephone number for people who prefer to use a conventional phone.

The WISP will become a competitor with the Internet services and so the WISP's pricing must be competitive. The third party service companies understand this and offer their service to the WISP at a low cost. In addition there is a lot of competition between third party service providers, which also helps to keep the cost low.

7.2. Third party TV services

WISP customers who live in rural areas usually have no cable TV and some customers are out of range of the antenna for over the air TV channels. The only TV service they have access to is satellite TV, however that service is expensive as the providers will only bundle many channels that the customer does not want with the few that the customer does want, and charge a high price for the bundle. The expensive bundling strategy is the reason why customers will change to another provider if an alternative is available. This is good news for a WISP because it is very easy for a WISP to get customers who currently have a satellite TV service. The WISP can offer a much lower cost with a streaming TV service, called IPTV, and provide only those channels that the customer wishes to pay for. The WISP can choose the services of several different streaming TV providers. The WISP can brand the service and select several options to offer customers. Website TV streaming services such as Amazon or Apple TV have two limitations. First they don’t have the local TV channels with local news and local weather that people want to see, and second they have some free channels but charge a subscription per channel for many channels, which can become expensive if several channels are selected.

The WISP can search on the Internet and find suppliers; one example is called WISPTV (http://www.wisptv.com/) that are geared towards providing a white-label TV service for smaller WISP businesses. The features offered by WISPTV are as follows.

- Made for all, Live TV + DVR made for rural and wireless Internet Providers.
- All things TV!, News, Top Shows, Sports, Free Classics and More.
- The best movies, Latest Pay Per View Movies on Demand.
- Updated daily, Fresh & Live Content Added Daily: Shows, Sports, News, Weather, Movies.

The WISP can speak to individual suppliers, or meet several suppliers at a WISP trade show, such as WISPAPALOOZA (https://preseem.com/wispapalooza/) and WISPAMERICA (https://wispaevents.org/), which meet every year.

The WISP should speak with several providers to find the best fit for the WISP’s business. The white label services require the WISP to take responsibility for the service as it carries the WISP’s brand. There are affiliate programs when the WISP refers customers for a third party service where the WISP might receive a monthly payment. Affiliate programs will be responsible for customer support and so reduce the burden on the WISP. The benefit of providing TV services is that they offer additional recurring revenue from established customers.

7.3. Third party telephone services

There are many Internet telephony service providers (ITSPs) offering IP phone services. The IP phone service uses a voice over Internet Protocol (VoIP) called SIP-trunking. This is based on the Session Initiation Protocol (SIP). The customer receives an IP phone handset that is connected to the premises CPE via the wireless router and receives a phone number that can connect to any other phone. Some service providers offer a white label service for the WISP to brand while other providers offer an affiliate program whereby the WISP receives one payment or a monthly payment for adding the customer to the providers network. If the WISP is branding a white label service then the monthly income will be higher however the WISP is responsible for the service. If the WISP joins an affiliate program the payments are lower however the provider assumes responsibility for the phone service.

VoIP vendors such as Nextiva (https://www.nextiva.com/) offer a comprehensive and reliable service and sell the service to customers through their website. Nextiva also has an affiliate program that permits a WISP to sell the VoIP service to the WISP's customers and make money. Nextiva offer the WISP a commission for customer acquisition and do not share recurring revenue. Some of the features that Nextiva offers affiliates are listed below.

- Top selling products & high commissions.
- Payments on both leads & sales.
- Earn $100 per qualified lead plus $100 per phone line sold.
- Dedicated affiliate team.

Like any other third party services, the more time that the WISP invests into the service the more money the WISP is likely to make.

7.4. Third party security services

Many small security businesses install alarm and video surveillance systems for residential and business properties. The alarm connects back to a central office via a phone line where it is monitored by security staff, and the video surveillance installation records the video on a digital video recorder (DVR). Security businesses have been delivering alarm-monitoring services for many years. Recently a new generation of security technology has been developed which uses the premises Internet connection to stream the camera video to a digital video recorder in the cloud, called a network video recorder (NVR). The security system eliminates the traditional door alarms and movement detectors with software that detects movements on the video feeds in real-time.

One video surveillance company that provides networked video surveillance services is called Eagle Eye Networks (https://www.een.com/). This company has a reseller program that offers recurring revenue paid to the WISP for each customer that the WISP installs. Eagle Eye offers support for resellers.

- Training & Certification;

  In person, hands on training to more easily implement Eagle Eye Network systems.

  Take part in online training seminars, product webinars and best practice sessions.

  Pre-launch information about new products and features.

  Receive discounts for multiple attendees or earn free registration at the annual reseller conference.

- Marketing & Sales;

  Get pre-qualified opportunities through a wide-range of marketing efforts.

Product updates, roadmap sessions, pilot programs, and other helpful sales tools.

Access to online marketing tools including; brochures, social media/campaign content, datasheets, and videos.

- Service & Support;

A unified dashboard; that manages, monitors, troubleshoots, & adjusts the customers cloud video surveillance accounts.

Access via phone or online to the Eagle Eye Networks industry leading support team to help better serve the customers.

Improve customer satisfaction and add recurring revenue through Eagle Eye Network Premium Support offerings.

The WISP has to install IP cameras at the customer's premises and configure the cameras with a wireless network that connects the cameras through the WISP's service to the video surveillance service provider.

There are many similar video surveillance service providers and the WISP should search for contacts via Google to compare the reseller deal that is offered.

7.5. Offsite data storage for business installations

One of the services that most IT firms offer is daily or hourly offsite data backup for security. Offsite data backup is very important for many types of business such as lawyers and accountants as client data is essential for business operations. There are two situations where offsite backup will save a customer's business. The first is a fire or building damage at the customer's premises, which will destroy computer equipment. The second situation is a ransomware attack to the business computers where the problem can be solved by reformatting the hard drive, reinstalling the software and reloading the data from the off-site data backup.

The WISP can offer the offsite data backup service to customers with a data circuit provided by the WISP using servers installed at the network operations center, and configuring the customers server to copy data files to the WISP's server periodically. The WISP can partner with IT businesses that provide their business customers with IT services so that the IT companies become resellers of the WISP's offsite storage. This is an advantage for IT companies as most do not have a data center and have to contract with a third party for data storage. The WISP has data center infrastructure in the network operations center for the administrative software and network equipment, so that most of the overheads are already paid for.

Rather than install servers at the network operations center the WISP can take advantage of third party services. At the low cost end of the scale the WISP can rent a virtual private server (VPS) (https://www.ionos.com/servers/vps) for as little as $2 per month and for that low price the WISP can backup data onto two servers for added reliability. A virtual private server is actually part of a server that is operating in virtual machine (VM) mode so many customers share the server. At the other end of the cost scale the WISP can contract with Amazon AWS (https://aws.amazon.com/) or Microsoft Azure (https://azure.microsoft.com/en-us/) for high reliability cloud storage that expands as required.

7.6. WiFi Hotspot services for business installations

The WISP will find that many types of business customer who contract with them for Internet service will also want an on-demand Internet service for their customers and guests, which is additional income for the WISP. Some of the businesses that want to provide Internet for their customers are listed below.

- Hotels and motels.
- Retail businesses, stores, etc.
- Airports.
- Service businesses, gyms, etc.
- Coffee bars, restaurants.
- Campgrounds and RV parks.
- Internet cafés.

These businesses have one common requirement; they want to provide Internet for their customers, but want to exclude people who are not their customers. The WISP has to provide two additional components for the network installation.

- Wireless access points that are not encrypted and cover the area of the property where the business customers need Internet access.
- A captive portal with login page and a means of generating access codes for customers.

Businesses have many different requirements for access codes, listed below.

- Code of the day. The business posts a daily free Internet access code for use by any customer. The code is multi-user and is valid for one day. The business has a list of codes provided by the WISP and posts a different code each day. The access code determines the maximum data download and upload speed so that the available bandwidth can be shared between many customers.
- Two-tier access. The two-tier system is popular with hotels. Hotels and motels have to offer free Internet for guests so a daily free multi-user access code is provided for guests. The free access code has slow maximum download and upload speeds. The captive portal login page explains to guests that if they want high speed Internet they can purchase via the captive portal using a credit card.
- Charged Internet access. Campgrounds and RV parks are at remote locations because their customers want to enjoy the peace and quite of the location. Remote locations don't have 4G-phone coverage but visitors want to remain in contact with friends and family. The WISP can provide Internet for the

campground or RV Park through a point-to-point wireless link or satellite Internet link, and then install a gateway at the site that provides a captive portal with a login page. The WISP also provides a method to charge credit cards to purchase Internet access and also a method to print vouchers with Internet access codes for cash sales.

The WISP can choose from several different products to provide the captive portal that includes credit card billing and voucher printing for cash sales. Guest Internet (www.guest-internet.com) manufactures popular products for a wide range of Hotspot service applications. The smallest product is suitable for a coffee bar or Internet café while the largest product is suitable for a sports stadium or airport with thousands of people connecting to the Internet. Guest Internet products have all the features that a WISP requires, including the configuration of multiple rate plans so that the business customers can choose low cost or high bandwidth access. Guest Internet products also provide a gateway to a credit card processor and can print multiple vouchers for cash sales.

7.7. Other types of IT services the WISP can offer to businesses

Many WISP’s will be providing Internet services in rural areas and part of the WISP customer base will be small businesses. Small businesses need IT services and rural area businesses frequently do not have access to an IT service firm. When the rural WISP has small business customers the WISP has the opportunity to offer a range of IT services for customers. Some IT services that the WISP can offer are listed below.

- Selling and installing computers and software.
- Training staffs how to use computers and software.
- Installing local area network (LAN) infrastructure at the customers premise.
- Cloud services to move the customer’s applications software to the cloud.
- Monitoring the customers LAN network for equipment failures.
- Providing a 24x7x365 support and repair service.

The WISP’s field service technicians will all be familiar with the services listed above and will have no problem providing these services. By offering IT services the WISP may make more productive use of technical staff and increase the revenue per customer.

7.8. Summary

The key points or take-a-way's that a WISP entrepreneur should remember when planning to provide additional services for customers are listed below.

- Capturing a new customer costs more then up-selling to an established customer which will increase revenue per customer.

- Offer subscribers a TV service over the Internet that costs much less then satellite TV.
- Provide subscribers with an Internet connected phone that will cost less than a subscriber wire-line phone.
- Subscribers can install a cloud based video surveillance system for home or business security.
- Business customers will appreciate the security of providing them with off site data storage.
- Many business subscribers need an on-demand Internet service for guests and visitors and the WISP can install this service at the business customer’s premises.
- A WISP can add an IT service role for rural business subscribers who do not have access to other IT services.

8. Transition to a LEO satellite backhaul

8.1. Supply and demand for Internet services

There is a huge demand for Internet access in industrialized and developing countries, however a part of the Earth's population has no access to the Internet. There are reasons listed below why a significant proportion of the world population cannot get Internet access.

- There are large areas that have no communications services; there is no Internet service, no mobile phone service, no fiber, no DSL and there is no WISP service as a WISP requires a copper or fiber Internet connection.
- There are geo-stationary satellite services available for some areas of the earth however many people in the areas without terrestrial service cannot afford the cost of the geo-stationary satellite service; furthermore they have no bank accounts or credit cards so would not have a method of payment.
- Low earth orbit (LEO) Internet satellites are being launched and already provide a service in some parts of the world. LEO satellites have the same problem as geo-stationary satellites; their cost is too high for many people who live in the large areas that have no Internet service of any type.

There are a few WISP's located in areas where there is no Internet backhaul connection who use geo-stationary satellites to provide Internet service for their customers, however the bandwidth of the satellite antenna is limited, which limits the number of customers that the WISP can serve. When LEO services become available the available bandwidth will be higher than geo-stationary satellites for a similar cost.

It is likely that some WISP customers in the USA will switch to LEO satellites, as the service will offer faster Internet for a slightly higher cost. In the parts of the world that have no Internet access most potential customers cannot afford the satellite services. WISP's can use LEO satellites to provide the Internet connection and then share the service between many users. A WISP in a region without Internet and with potential customers who are economically limited in what they can pay, is able to provide a 2Mb/s Internet service for $2 per month. Such a WISP can provide a service for 300 people connected to one LEO antenna with a low contention ratio, more with a higher contention ratio.

The next figure shows areas of the earth where rural communities have no or limited access to the Internet. Fire4 Systems Inc. provided the regional information from sales data of WISP products that control network access with on-demand voucher Internet sales for cash payments, a product line that is popular in these areas. This method of selling Internet using on-demand vouchers is popular because customers can purchase vouchers with cash payments. The majority of the population in these areas cannot afford the cost of a satellite service and don't have bank accounts or credit cards to pay for the service. Some urban areas that are within the circles do have DSL and 3G/4G Internet access however the current cost is high for the people who live in these areas. In order to provide a lower cost Internet service in these urban areas WISP's share a DSL circuit between many users for a low monthly cost per user. There are no opportunities for WISP's in large areas like Russia and China and several smaller countries like Cuba as the governments only permit state provided and censored Internet access.

When the LEO constellations are completed then LEO wireless Internet will be available at any point of the earth. In the parts of the world where customers can easily afford the service, like North America, then LEO services like Starlink will be competing with other services of similar performance and cost. In the USA there are still rural areas without any type of Internet service however the people in those areas can afford the cost of Starlink if they wish to have Internet access.

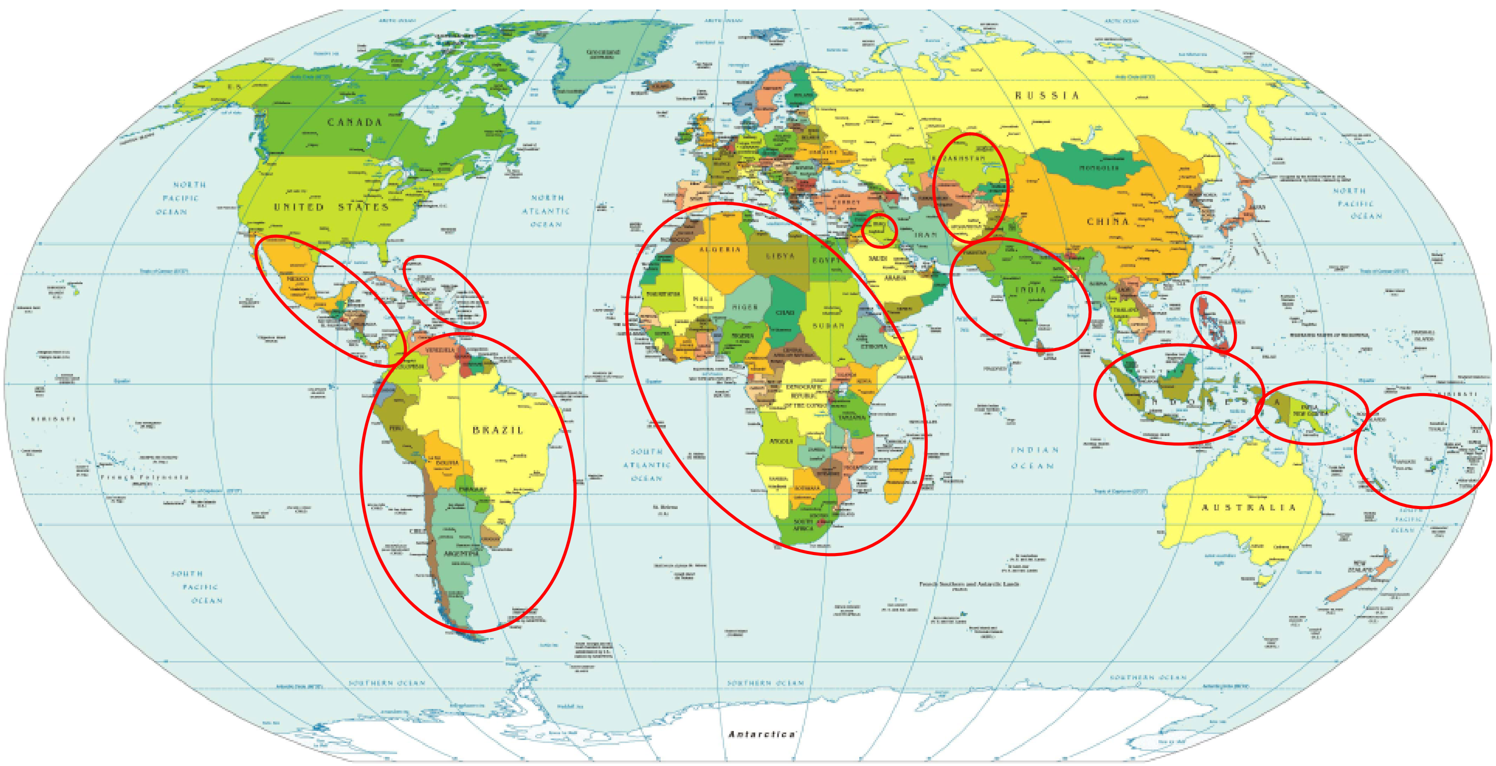


Figure 8.1.1. Approximate areas of the earth are circled where there is no or limited Internet access for rural customers. (Data compiled from Fire4 Systems Inc. sales records 2010 to 2021).

In many parts of the world that are indicated on the map there are no Internet services in rural areas and limited Internet in urban areas. The cost of LEO satellite services is too expensive for most people who want Internet access in these areas. A LEO satellite service however does provide an opportunity for a WISP to provide Internet access for many people, and for a low monthly cost that is affordable for the rural demographic who have no alternative means to access the Internet.

In the parts of the world that are indicated on the map, a LEO satellite service is the only possible Internet backhaul for WISP's who want to provide a service for customers. The introduction of LEO satellite Internet services will create many thousands of new WISP's who will have chance to provide a low-cost service for customers and make money. WISP’s that are already established in the areas indicated in the figure operate with a different business model to WISP’s in the USA.

- The Internet backhaul is divided between many more customers than a WISP would do in the USA, offering a lower performance service for a lower cost.
- A few customers with a higher income are monthly subscribers.
- The majority of customers choose the on-demand mobile broadband service rather than a fixed broadband subscription for reason of cost.
- Commercialization of the service is predominantly through cash payments.

The availability of LEO satellite services for enterprises to resell access will open low-cost Internet access for millions of people around the world and the majority of Internet users will be customers of new WISP's that were started to take advantage of the LEO satellite Internet services.

8.2. Comparing geo-stationary and LEO satellite technologies

Geo-stationary satellite Internet has been available for many years. Initially the service was very expensive and the customers were businesses that could afford the cost of the service. The marine industry has relied on VSAT and Intelsat to maintain data communications with merchant shipping around the globe. Several services are available for residences and businesses and the most popular is the HughesNet service.

LEO satellite networks have been available for phone services but the ventures were limited in success, in part due to the high prices charged. LEO satellites providing low cost Internet services are a recent development and appear to provide a very popular service. However the LEO satellite business must make the huge investments to ensure that the service is successful.

The characteristics of geo-stationary satellite services are listed below.

- A satellite in a geo-stationary orbit rotates at the same speed as the surface of the earth above the equator and so remains at a fixed point in the sky, a ground parabolic antenna can therefore remain fixed to the location of the satellite.
- One satellite communicates with ground antennas over an arc of the earth’s surface.
- As the satellite is stationary above the equator then it can cover the northern and southern hemispheres however the satellite antenna beams are focused on the areas of land mass with denser populations to maximize the number of customers.

- As the satellite is above the equator antennas in the extreme northern and southern hemispheres of the planet see the satellite very low on the horizon, and as the radio signal passes a greater distance through the atmosphere the quality of the signal is reduced.
- All customers connect through one large satellite and so the bandwidth available per customer is small. There will be a maximum number of customer antennas that each satellite can support due to the limited data throughput capacity of the satellite.
- The satellite geo-stationary orbit is 22,000 miles above the equator, the time taken for the transmission to the satellite and back to earth is 236ms, and the total latency of Internet access is approximately 300ms to 600ms.
- The geo-stationary satellite operators put a data cap on monthly use due to the limited bandwidth and impose additional charges when data use exceeds the cap.

Geo-stationary satellite firms are listed below. Note that these firms do not offer complete global coverage.

- HughesNet.
- Viasat.
- Skycasters.
- VSAT.
- Intelsat.

Several firms have planned LEO satellite constellations to provide Internet services but at the present time Starlink is currently the only LEO satellite business that is operational, and is available only over part of the northern hemisphere. Starlink has published technical information about the satellite service and network operation but very little information is available about other LEO satellite systems. Characteristics of the Starlink low earth orbit (LEO) satellites are listed below.

- At any one time a point on the earths surface has visibility of one to several satellites.
- Starlink planed to have a total of 12,000 satellites in orbit initially however now that number has been increased to over 30,000 satellites when the constellation is complete.
- Starlink is launching satellites every month, with 60 satellites per rocket launch.
- At the present time Starlink has satellites located in a number of orbital shells around the earth.
    - First shell: 1,440 satellites in a 550 km (340 mi) altitude shell at 53.0° inclination.
    - Second shell: 1,440 satellites in a 540 km (340 mi) shell at 53.2° inclination.
    - Third shell: 720 satellites in a 570 km (350 mi) shell at 70° inclination.

    - Fourth shell: 508 satellites in a 560 km (350 mi) shell at 97.6°.

- As Starlink satellites are close to the earth they require less transmission power than a geo-stationary satellite and are therefore much smaller.
- Starlink customers report data download speeds exceeding 150Mb/s with a latency of less then 30mS.
- Starlink has no monthly data cap so no additional charges are imposed.
- Each customer's antenna will be programmed to operate at a specific longitude and latitude coordinate.
- There is a maximum density of customer antennas per square Km due to the limited number of satellites overhead at any one time. Customer antennas that are close together will share data through the same satellite. As more satellites are launched the number of customer antennas that can be installed per square Km will increase.
- Starlink antennas are not directional as they communicate with satellites over a 180 degree arc of sky; the antenna used is a beam-forming phase array that can be directed electronically to any point in the sky to track the satellites.
- As LEO satellites have a low orbit then the orbital speed of a satellite is much faster than the rotation of the earth so a satellite will traverse the sky from horizon to horizon in a few minutes, the customer antenna will select a satellite that is close and switch between satellites as each moves overhead.
- Current Starlink customers are beta testing the service and Starlink restricts how the service can be used.
- The Starlink service is currently only available in the northern part of the USA, Canada and northern Europe and there is only a small fraction of the total number of satellites in orbit at the present time.
- The Starlink service requires approval for use of the communications frequencies in each country where the service will be provided, and it is approved in only a handful of countries at present.
- At present Starlink is limited to residential and small business use and cannot be used by WISP's as an Internet backhaul to sell Internet services. However the company stated that an enterprise service will become at a higher price.

LEO satellite competitors are listed below. Some LEO firms have gone through bankruptcy and then continued with new investors.

- SpaceX Starlink.
- Amazon Kuiper satellites.
- Kepler Communications.
- Northrop Grumman.
- Boeing.
- Lockheed Martin.
- Thales Alenia Space.

- Airbus Defense and Space.
- SSL.
- Globalstar.
- BAE Systems.
- Oneweb.

WISP’s may have to wait until 2024 or later before a LEO satellite service is available for use as a tower backhaul, however WISP's should begin thinking about using a LEO satellite service now so that current infrastructure investments will support future LEO satellite expansion.

8.3. Starlink technology

The Starlink satellite constellation will have more than 30,000 satellites when completed. The satellites will orbit in several orbital shells, each shell at a different altitude and with a specific inclination to the orbit of the earth. Each customer will have an antenna that can communicate with a satellite over approximately 180 degrees of the sky, and can swap the connection between satellites as each move across the sky. Each satellite will relay the customer connection to one of the many ground stations around the globe. Each ground station will have a high-speed connection to the Internet. Eventually there will be a laser connection between satellites so that a circuit is made through a mesh of satellites to minimize the terrestrial connection between the customer’s antenna and the ground station server location to reduce latency between points on the earth.

Although the number of satellites may appear to be large, there are few satellites for each arc of the earth’s surface. The density of satellites over the earth’s surface can be calculated as follows.

Calculate the area of the earth’s surface covered by each satellite.

- Total approximate area of the earth’s surface;
  - = 196.9 million sq miles.
  - = 510 million sq Km.
- Area per satellite;
  - = 196.9 million mi² / 30,000 satellites = 1 satellite per 6,562 sq ml.
  - = 510 million sq Km / 30,000 satellites = 1 satellite per 17,000 sq Km.
- Calculate the circle diameter of the earth’s area covered by each satellite;
  - D = 2 x root (6562 / pi) = 91 miles diameter.
  - D = 2 x root (17000 / pi) = 147 Km diameter.

Calculate the number of satellites over land at one time.

- Approximate area of the surface of the earths land mass;
  - = 57.5 million sq miles.
  - = 149 million sq Km.

- Ratio of land mass area to total area;
    - = 57.5 miles / 196.9 miles = 0.29.
- Number of satellites over land = 30,000 x 0.29 = 8700 satellites.

This number of satellites over land may be higher due to the selection of satellite orbits to increase the number of orbits over land areas. There will be a maximum data throughput for each satellite, which will limit the number of customer antennas within the area covered by a satellite. In practice the number of customer antennas can be higher as satellite orbits in different shells overlap to increase the density of satellites for an area of the surface. SpaceX has not released information about specific satellite orbits and customer antenna density limitations.

The next figure illustrates the orbits of satellites at different inclinations and in different shells.

Figure 8.3.1. Starlink satellite orbital inclinations, within shells at different altitudes. (Image copyright © SpaceX 2021).

Each satellite has a fixed orbit in space however the earth is rotating and so each satellite will be over a different landmass with each orbit of the earth. It is possible that any point on the earth might have two satellites overhead at any time due to orbital shells with different inclinations. The customer ground antennas will have a 180-degree visibility of the sky and so several satellites might be visible to the antenna. The satellites will move across the sky from horizon to horizon in several minutes as a low earth orbit requires a much faster orbital velocity that the speed of the earths rotation. The figure shown below illustrates the constellation of Starlink LEO satellites in orbit around the earth, within several shells, each shell at a different altitude.

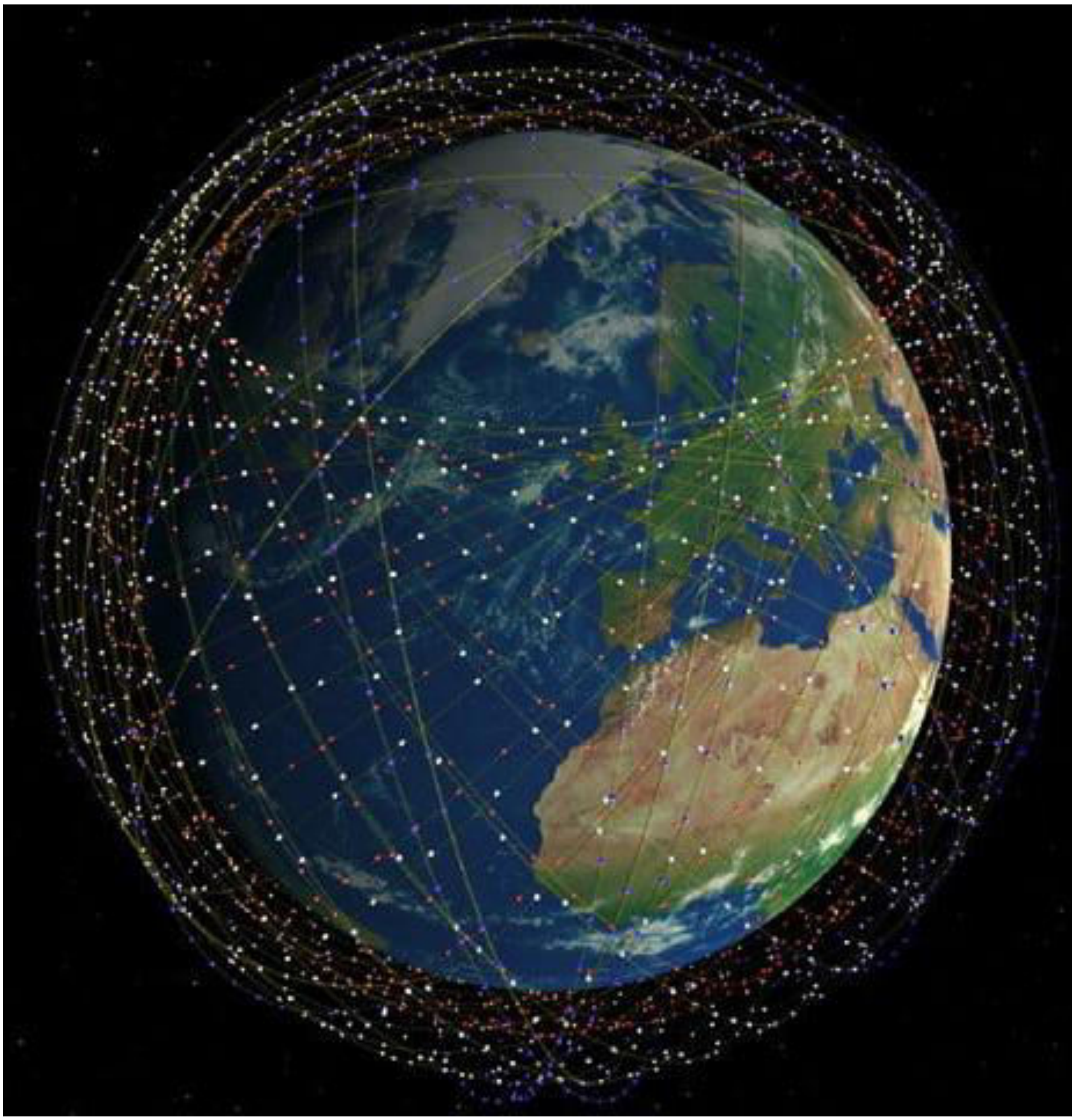


Figure 8.3.2. An illustration of Starlink satellites in orbit around the earth within several shells. (Image copyright © SpaceX 2021).

Starlink satellites are launched in batches of 60 satellites per launch. After the batch of satellites is in orbit each satellite is maneuvered into the correct orbital position. Satellites require positional corrections periodically to maintain the orbital position. Each Starlink satellite also has a positional booster to de-orbit the satellite if some technical failure occurs and the satellite will then burn up in the atmosphere. Starlink can replace satellites that have been de-orbited.

The following illustrations show Starlink satellites in orbit.

Figure 8.3.3. Starlink satellites in orbit. (Image copyright © SpaceX 2021).

Each satellite has a solar array to capture sunlight during the part of the orbit where the sun is visible. The electrical energy that is generated is stored in batteries to power the satellite during the part of each orbit where the earth blocks the sunlight. The expected lifespan of each satellite is in the range of 5 to 7 years. The space environment is harsh and dangers include electromagnetic radiation across all frequencies that may damage electronic circuits, and collision with micro-particles that may damage external components.

The next illustration shows the earth-facing antennas of a Starlink satellite.

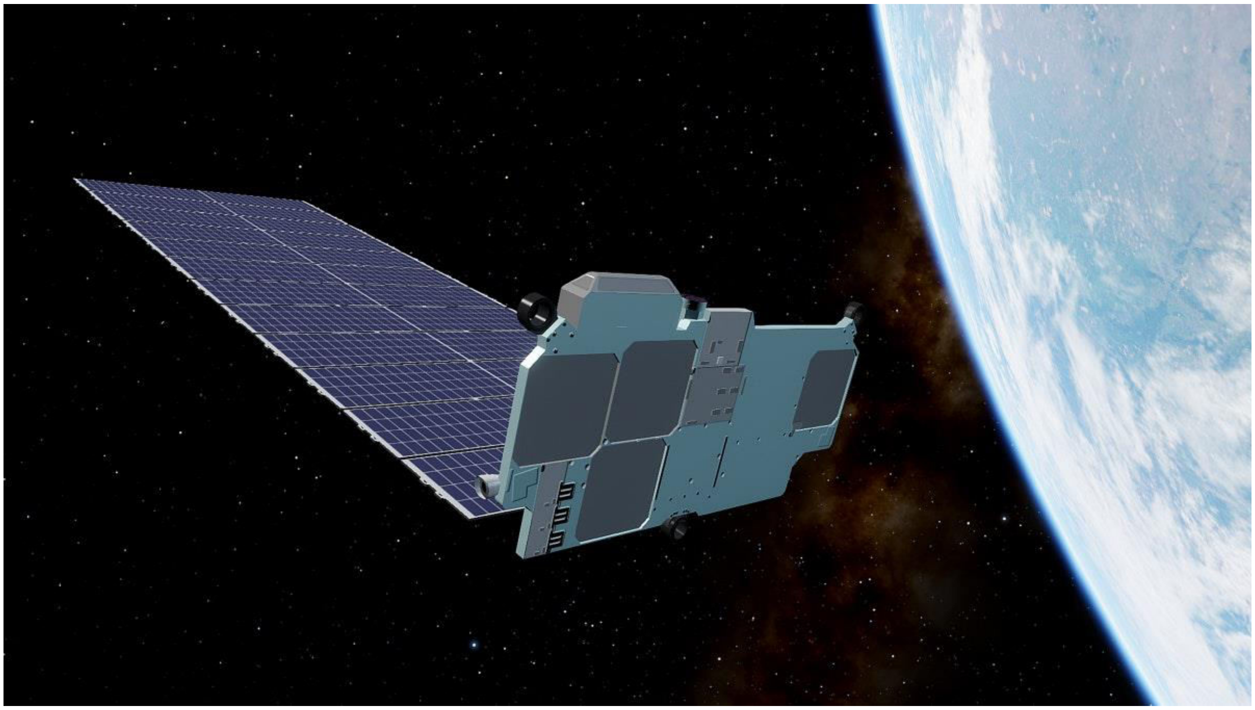


Figure 8.3.4. Starlink satellite antennas for transmitting and receiving from the customer antenna and to the ground station. (Image copyright © SpaceX 2021).

A customer Starlink antenna is shown in the next illustration. Each antenna includes a wireless router for installation inside the premises and a power over Ethernet (PoE) supply to power both the antenna and the wireless router. Starlink have stated that the cost of manufacturing this antenna exceeds the sale price of the antenna.

The antenna design shown will soon be replaced by a square antenna, which has a lower manufacturing cost.

Figure 8.3.5. Starlink customer antenna with wireless router and PoE injector (Image copyright © SpaceX 2021).

The Starlink customer antenna has a motor, which adjusts the attitude of the antenna. The antenna is a phase array beam forming design, which means that the antenna can be directed electronically over approximately 180 degrees of the sky. The beam-forming antenna was described in an earlier section of this book. The antenna must have approximately 180-degree visibility of the sky to ensure that it can connect with at least one satellite. If the antenna is installed in a location surrounded by buildings or trees then the antenna must be mounted on a roof or antenna tower to provide 180-degree visibility of the sky. The following photo shows a Starlink antenna mounted on a Rohm antenna tower to support the antenna above surrounding trees.

Figure 8.3.6. Starlink customer antenna mounted on a mast for a clear view of the sky (Image copyright © SpaceX 2021).

Starlink has ground stations located around the earth and each one has a high speed Internet connection. SpaceX has an agreement with Google to install Starlink ground stations at Google data centers. Each ground-station includes a cluster of several antennas like the one shown in the next photograph. As satellites pass over the ground-station a link is established to permit the satellite to relay data packets between the customer antennas within the range of the satellite and the ground-station antenna.

Figure 8.3.7. Starlink ground stations are installed around the earth; no information is available about the number of ground stations currently installed (Image copyright © SpaceX 2021).

A future feature of the Starlink constellation is the ability to relay data communications between satellites using a laser data link so that the greater part of the data path between two points on earth is between satellites in orbit rather then through terrestrial data connections. This feature will speed data communications between two points by reducing the latency time or delays of the transmission.

The next illustration indicates a laser data connection between satellites for a data circuit from London to New York. Instead of the data connection passing through undersea fiber optic cables, which have a high latency due to the large number of repeaters, the data connection is relayed through several satellites in different orbits.

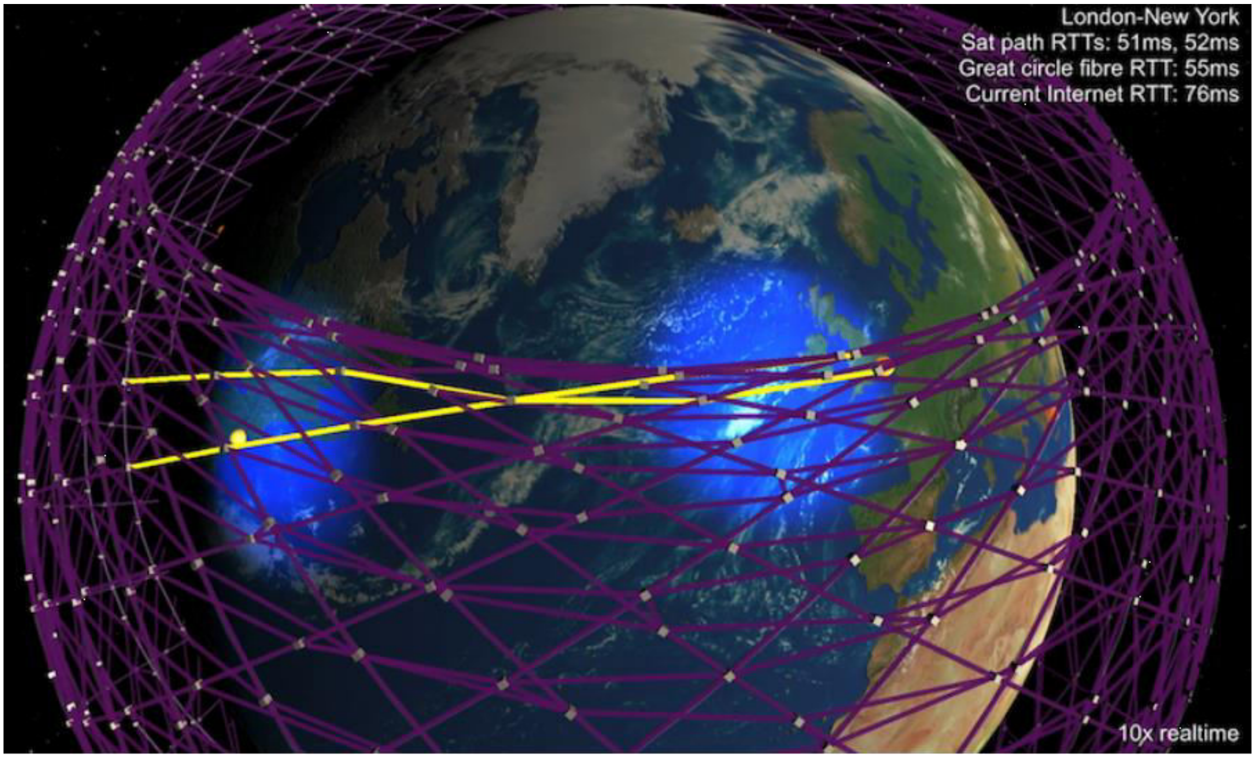


Figure 8.3.8. London to New York data connection; Starlink communication between satellites via laser to minimize high-latency terrestrial paths for each data link. (Image copyright © SpaceX 2021).

The operation of Starlink has to be approved in each country where it will provide service, as the frequencies used by Starlink require a license to authorize their use. At the time of writing Starlink has been approved by 14 countries and has pending license applications in many more countries.

8.4. Adding a LEO satellite backhaul to an operational WISP network

A WISP that has built a network with several PtMP towers, with each tower connected back to a NOC through a wireless distribution network has three methods to upgrade to a LEO satellite Internet backhaul.

The first method is to install the LEO satellite antenna at the NOC. There is little benefit installing two or more LEO antennas at the same location as multiple antennas will communicate through the same satellite, giving only a small throughput benefit compared with having only one antenna. A single LEO antenna installed at the NOC can augment the data backhaul capacity allowing more customers to be added to the network, and also provides redundancy in the case that a problem occurs with the principle fiber backhaul connection. The next diagram illustrates the installation of a Starlink antenna at the NOC.

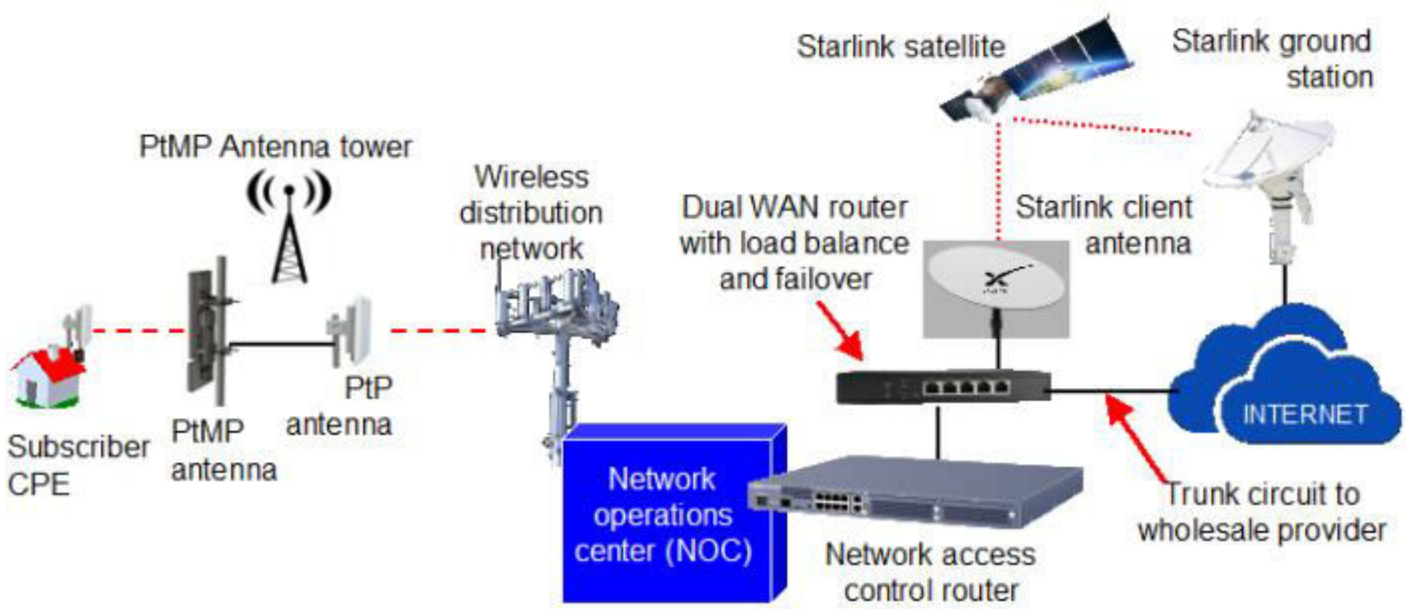


Figure 8.4.1. LEO satellite antenna installed at the NOC of an established WISP.

The WISP can obtain improved performance by installing a LEO antenna at each PtMP tower. Towers are spaced several Km apart and so each LEO antenna may communicate with a different satellite permitting each tower site to have the full backhaul bandwidth of 100+ Mb/s. The existing wireless distribution network to the tower can be maintained to increase tower capacity permitting the connection of more customers to that tower, and also add redundancy to the tower site.

There are two methods to implement and upgrade the WISP network when installing a Starlink antenna at each tower.

The first method requires the connection of the PtMP wireless access point to a load balancing router that routes the user traffic to both the wireless distribution network and to a VPN gateway to tunnel through the Starlink network via VPN back to the NOC to implement access control. This method has the disadvantage that a part of the customer traffic is routed to the NOC via the Internet for access control and therefore the NOC trunk circuit capacity has to be increased to correspond to the additional traffic carried over the Starlink network back to the NOC. The next figure illustrates the tower installation, where data is partly routed over the wireless distribution network to the NOC, and partly routed through a tunnel over the Starlink network to the NOC for access control. Maintaining access control at the NOC is not a satisfactory solution when the WISP adds Starlink antennas to increase the capacity of the network.

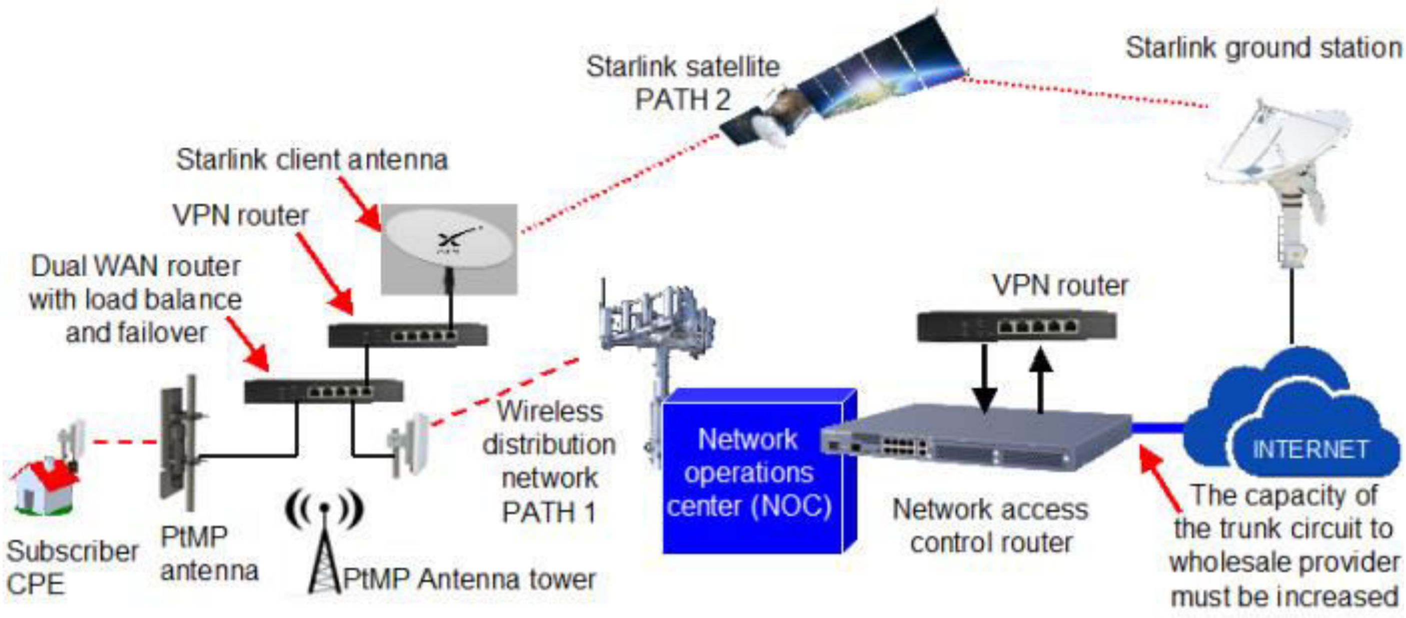


Figure 8.4.2. LEO satellite antenna installed at the PtMP tower with access control at the NOC.

The second method requires the installation an access control router at each tower. The access control router connects to a load balance router that routes customer data over both the Starlink network and the wireless distribution network back to the NOC, and from the NOC to the wholesale Internet connection. The load balance router shares the traffic load over the two circuits in function of the capacity of each circuit. The load balance router also has a failover function so that in the case that one-circuit fails; all traffic is routed over the remaining circuit. This network design requires no access control at the NOC.

Having access control at the tower simplifies the network implementation and also uses the available circuits efficiently. The network administrator has an additional workload due to programming several different routers, one at each tower. If the WISP chooses software that automates the programming of routers then the management of the network becomes very simple. The next figure illustrates the network design when a LEO antenna and access control router is installed at each tower.

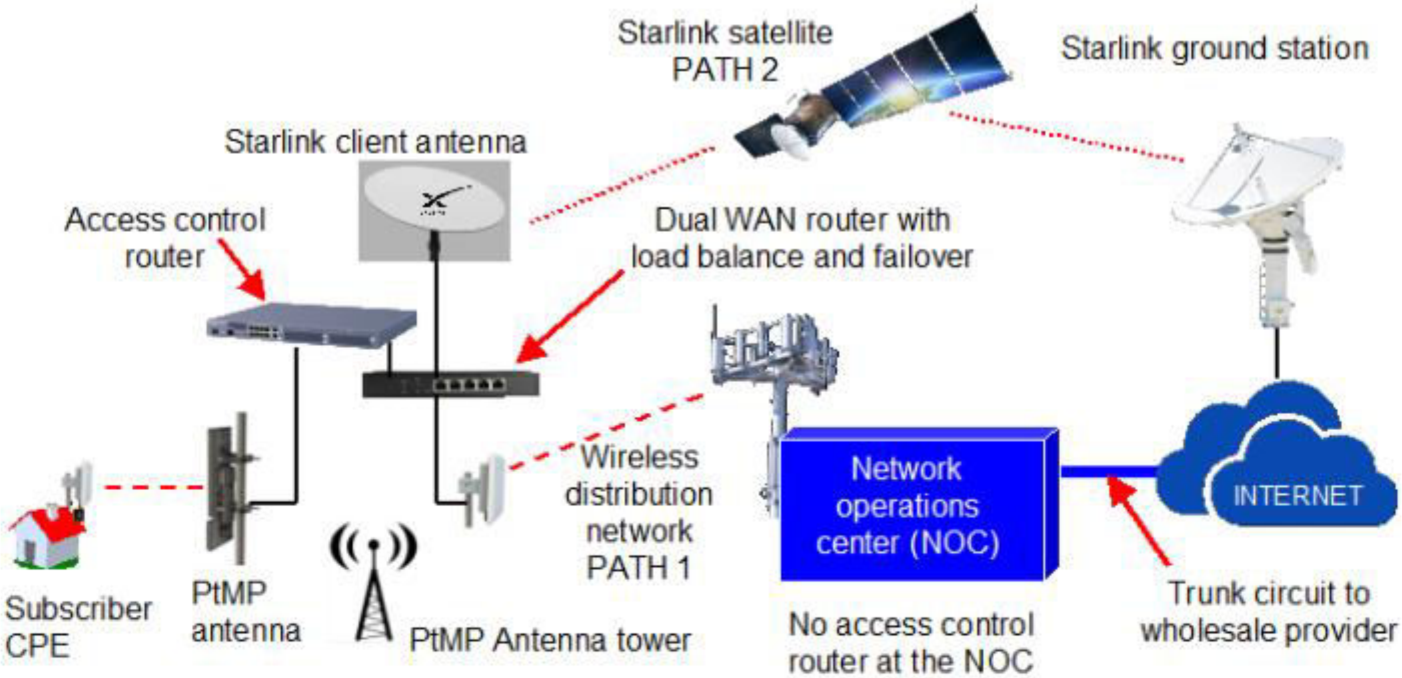


Figure 8.4.3. LEO satellite antenna installed at the PtMP tower with access control at the tower with dual WAN load balance and fail-over.

8.5. A network design for the start-up WISP using Starlink

An entrepreneur who starts a WISP business today has a limited radius of operation around the location where the WISP can contract a wholesale or even retail data connection to the Internet. The radius of operation can be up to 50Km depending on the facility to build multiple-hop wireless point-to-point links. If there is no Internet data connection then a WISP cannot be established. When LEO satellite services become available globally then entrepreneurs will have the opportunity to build a WISP anywhere in the world. A terrestrial Internet service connection is not required. The use of LEO services does place some restrictions on the network design, as listed below.

- LEO satellite antennas cannot be grouped together, they must have a minimum distance separating them; installing the LEO antennas at each PtMP tower site is a good solution as towers are spaced a few Km apart.
- The access control router is installed at each tower between the PtMP wireless antenna and the LEO antenna as part of the equipment configuration; therefore the technical person responsible for network configuration must manually configure multiple small routers, each router is configured for the customers served by that PtMP tower. Alternatively the WISP can install management software that automates the configuration of multiple routers.

The next diagram illustrates the network design with a LEO satellite antenna installed at each PtMP tower.

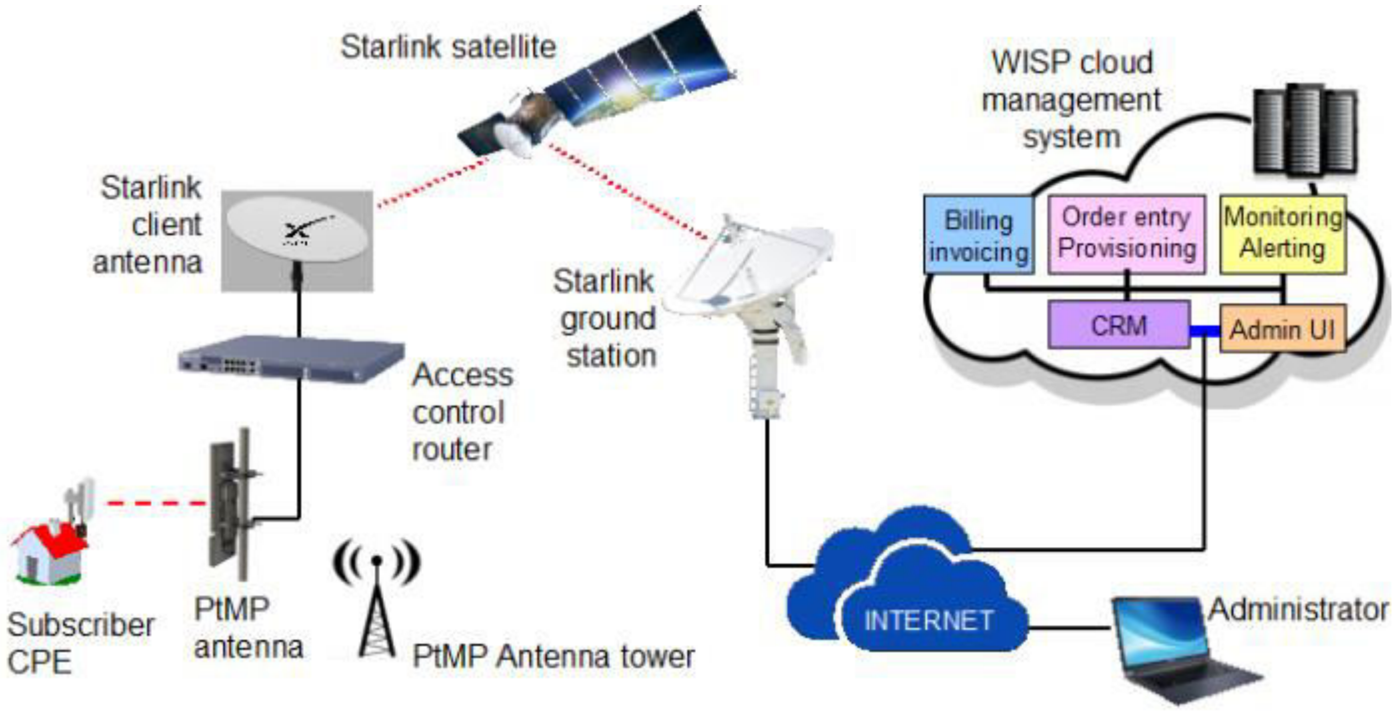


Figure 8.5.1. LEO satellite antenna installed at the PtMP tower with access control at the tower.

When an entrepreneur plans to start a WISP business in future then installing a LEO satellite antenna on each PtMP tower together with the access control router in a distributed network design has a series of business benefits when compared to the centralized NOC network management. The benefits are listed below.

- When LEO satellite services are available around the globe then a WISP company can be established anywhere.
- Building a NOC is not necessary, which eliminates a large initial investment.
- There is no wireless distribution network between each PtMP tower and the NOC, eliminating a considerable investment.
- As the only infrastructure build-out is the PtMP tower then the WISP can start in business much faster, speeding return on investment.
- The WISP can install business management software on a cloud service such as AWS, or else contract with one of the cloud management services.
- The reliability of the Internet service provided for the customer is improved, less equipment to fail and backup systems are required only at the tower.

- The WISP carries fewer inventory parts, which reduces investment; the only inventory items required are customer CPE kits and equipment to build and repair towers. Equipment for servicing the wireless distribution network and NOC is eliminated.
- Fewer technical staffs are required and some operating costs can be eliminated due to the simplified network design, installation, support and maintenance requirements.
- The WISP administrator uses an Internet connected laptop to manage the business from anywhere that has an Internet connection.

The next figure illustrates the tower installation with a LEO satellite backhaul. It may be necessary to install multiple PtMP wireless access point in order to cover the area desired.

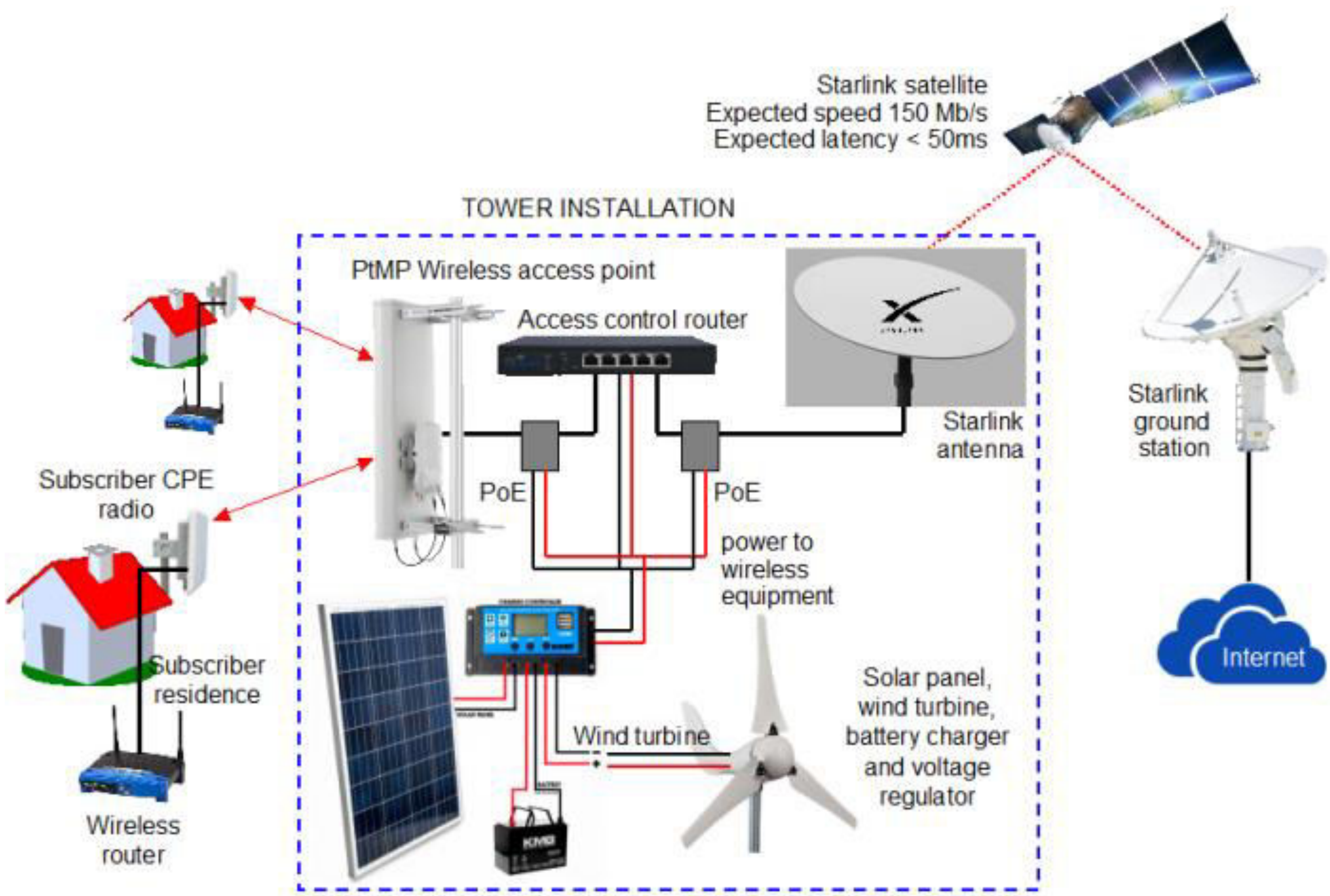


Figure 8.5.2. LEO satellite antenna installed at the PtMP tower with power generation for the equipment.

Network administration requires additional effort programming multiple access control routers. The WISP must maintain a list of subscribers at each tower and program the access control router for authentication and rate-plans of those subscribers. If the WISP chooses to implement a WISP management system that automates the programming of access control routers then distributed access control has no additional overhead for the WISP. Although few WISP administration software products support distributed access control management currently there are cloud products that were designed for a distributed management environment. It might be possible for a WISP who has programming skills to modify open-source management software for automation of distributed access control routers.

PtMP towers that are built in remote locations will not have electrical power and so infrastructure must be added to power the tower equipment. Generating power for the tower equipment has been described in a previous section. When a Starlink antenna is installed the power requirements are increased considerably as a Starlink antenna consumes much more power then a PtP backhaul antenna. The capacity of power generation should be increased to 500 Watts or higher. A solar array and wind turbine are installed as the sources of power and energy is stored in a battery. The battery storage should be planned to power the installation for 100 hours without charge, which is approximately 4 days of use. Vendors of tower power systems will give advice about the characteristics of the components to provide adequate power.

8.6. WISP network administration using LEO satellite backhauls

The WISP can choose how to implement the management automation of the network with LEO satellite Internet access at each tower. The approach recommended here is to have billing and network monitoring software installed at a central site or use a cloud service and configure each tower access control router for authentication, rate-plan settings, activation and deactivation in case of non-payment. A record of customers associated with each tower facilitates the individual access control router programming.

The WISP can select software or a cloud service that has the facility to automate the control of multiple access control routers while maintaining a record of customers who are authenticated by each router. WISP software can be hosted on a cloud service such as Amazon AWS or Microsoft Azure.

Routers have three types of remote interfaces, listed below.

- Command line terminal.
- Graphic user interface (GUI).
- Application program interface (API).

The router is programmed by adding scripts which are command lines of instructions that tell the router how to process incoming data streams. Scripts can be entered via the command line interface and some routers provide a graphic user interface (GUI), which will facilitate entering scripts that take action on customer data. Scripts can also be downloaded and installed using the API interface.

A WISP can program routers manually by connecting remotely to each router command line terminal or GUI interface to enter scripts. Automation systems will download scripts using the API interface. Initially scripts must be added to the router using the command line terminal or GUI to enable the API interface for remote access. Once the API interface is enabled the management software can communicate with the router to configure the customer access control rules.

The next diagram illustrates a WISP administration software or cloud service that automates the interface with each access control router.

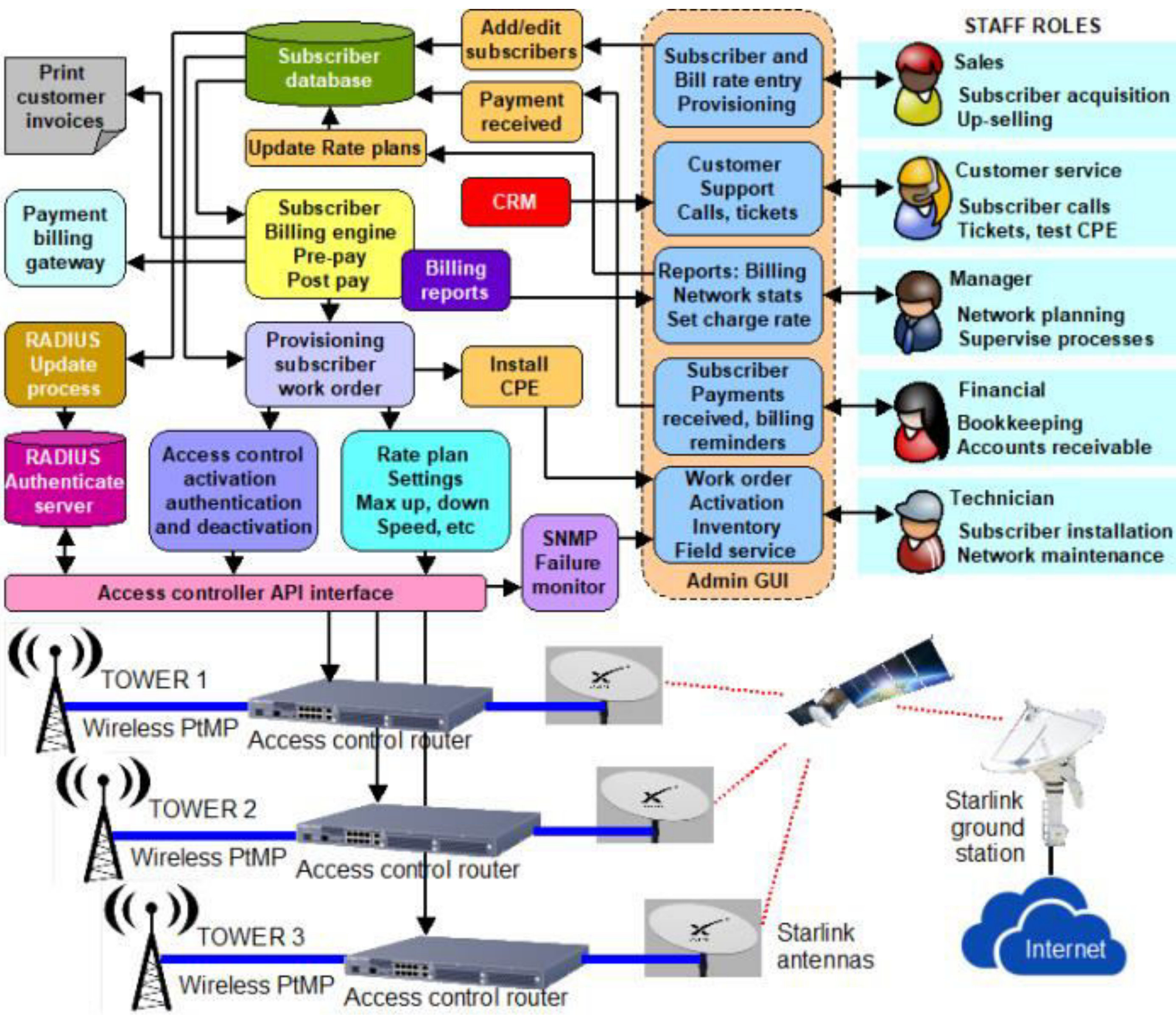


Figure 8.6.1. Administration software access control automation of multiple towers, each with a LEO backhaul.

There are six points of contact between the WISP management software and the interface API of the router that is selected for configuration.

- Configure the customer authentication method; this can be as simple as setting the CPE MAC address for simple authentication, or configuring the PPPoE server that will interface with an external RADIUS authentication server.
- Configure the SNMP agent for monitoring.
- Set the rate plan for each customer accessing the Internet through the tower site.
- Activate the customer allowing the customer to access the Internet.
- Deactivate the customer if the account is past due then redirect the customer to a CRM captive portal page.
- Poll the SNMP agent periodically to verify that the device is alive and gather operational information.

Each time that a customer opens a connection with the access control router the CPE will send the authentication credential to the PPPoE server, which will then authenticate the customer via the external RADIUS server, by passing the authentication key for validation.

The features listed are essential to fully automate the access control router functioning. Each WISP management system determines the access control automation specifics. Some systems may implement a partial list leaving some router programming for the WISP technician. Some systems may include additional features not described in the list above that improve performance of the access control process and add functionality.

8.7. New opportunities for WISP's that adopt LEO satellite services

An established WISP can begin to transition to Starlink when the service becomes available where the WISP is located. As of this writing satellite coverage is available only in the northern part of North America and countries in Europe, such as the UK. Some countries have satellite coverage but their government communications departments have not yet approved a license for Starlink to begin offering the service to customers.

In some parts of the world such as North America, WISP customers can afford the cost of the Starlink antenna and monthly subscription so the WISP's will see Starlink as a threat. Starlink is likely to take some of their customers. Those WISPs will also see the opportunity to expand networks into remote rural areas where they are not able now because there is no wholesale Internet access service but there are prospective Internet service customers who cannot afford the cost of the Starlink antenna and service.

In other parts of the world where there is no access to a wholesale Internet connection then a WISP can set up in business with Starlink, as there will inevitably be a pent-up demand of potential customers seeking an Internet access service. Starlink will empower entrepreneurs who would like to start a WISP business but are currently not able due to lack of backhaul infrastructure.

People who start WISP businesses in areas like North America are usually technically well qualified, with years of IT experience. They have qualifications such as certifications from router manufacturers, and have the capital required to start the business. People in many other parts of the world don't have the same good fortune; there are few IT jobs for them to gain experience, no access for formal technical training programs and very limited access to capital to start a business. In order that entrepreneurs in many parts of the world can start WISP businesses the following criteria for the WISP technology are essential.

- Extensive technical knowledge should not be required, the WISP system components should be very easy to connect and use, sometimes called plug-and-play technical solutions.
- The technical solution should be frugal so that the minimum amount of investment is required to start a WISP business.
- The technical solution should have a low operating cost, in the range of cents per subscriber per month.
- The economics of the business should permit providing a very low cost Internet service for a population with economic limitations where the charge will be in the range of a few dollars per month.
- The WISP should offer mobile broadband in addition to fixed broadband as potential customers with limited economic means will use low cost smart phones as Internet access terminals and seek locations where mobile broadband is offered. The cost of installing fixed broadband CPE equipment at the customers premises may be too high for the customer.

The criteria for the WISP management system for developing regions of the world are listed below.

- Must have the essential functionality for provisioning new customers, billing customers, monitoring network performance and alerting of network failures.
- Ideal to have an API Interface with popular routers for access control configuration that does not require learning the router command language to prepare configuration scripts.
- Where a PtMP wireless access point supports a router programming language (e.g. Mikrotik) then configure the product to serve as the access controller for customers who are assigned to that wireless access point.
- Must function with any type of PtMP wireless access point and CPE wireless unit.
- Should have multiple authentication methods for flexible configuration, including CPE MAC authentication, and a RADIUS server for PPPoE or WPA2-enterprise authentication.
- The operating cost per subscriber must be in the cents per month range, not the dollars per month.
- The billing system should support both fixed broadband monthly subscription billing and mobile broadband on-demand billing.
- The technical solution must be comparable with both a centralized NOC configuration and also a distributed configuration with a LEO satellite antenna at each tower to permit a WISP to set up in business anywhere in the world.

- The initial network investment must be the lowest of any system available in the market.

8.8. Summary

The key points or take-a-way's that a WISP entrepreneur should remember when planning to transition a WISP network to a LEO satellite service backhaul at each tower are listed below.

- LEO satellite technology offers better performance than geo-stationery satellite technology, faster speed and lower latency.
- Large areas of the planet do not have access to any Internet broadband service and LEO satellites are the only solution that has the data speed and low latency for a WISP to start in business.
- LEO Internet service from Starlink is already available in some parts of the world and Starlink has a date for global coverage.
- The Starlink LEO Internet service is not yet available for WISP's to use as an Internet backhaul but WISP’s should plan current infrastructure investments so that an enterprise version of Starlink can be incorporated.
- A process has been shown that can be used to upgrade an established network to add a LEO satellite service.
- There is a network design plan to build a WISP network from scratch using a LEO satellite service.
- Automation helps to manage a network when a LEO satellite backhaul is installed at each tower.
- There are new opportunities for WISP's who adopt Starlink.

The next chapter describes a technical solution that meets the criteria listed above and explains the economics of the solution ready for the WISP’s business plan.

9. A WISP start-up project

9.1. A WISP start-up plan with limited investment and limited technical knowledge

Most of the Wireless Internet Service Providers (WISP's) around the world are located in the rural areas of countries where the incumbent telecom companies do not provide an Internet service; in some cases not even a wired or wireless phone service.

Many people in rural areas of the USA rely on WISP's to provide their Internet service because the large telecom companies do not want the expense of providing an Internet connection to customers in rural areas. WISP's in the USA offer a service to rural areas only in locations where they can get access to a wholesale fiber Internet service. The USA has millions of people who don't have access to an Internet service. The FCC states in the Eighth Broadband Progress Report: *"approximately 19 million Americans, 6 percent of the population, still lack access to fixed broadband service at threshold speeds. In rural areas, nearly one-fourth of the population, 14.5 million people, lack access to this service".*

https://www.fcc.gov/reports-research/reports/broadband-progress-reports/eighth-broadband-progress-report

Geo-stationary satellite services are available for people in the USA but the cost of these services is beyond the budget of many people. Internet service can be obtained from a mobile 4G network when the customer is in range of a 4G tower, however many rural areas lack 4G coverage. There are a lot of opportunities in the USA for entrepreneurs who want to start a WISP business with reasonably priced services for rural customers.

People who live in rural areas, and even some urban areas, in many other parts of the world are in a much worse situation than people who live in the USA; they do not have access to any type of Internet service. It is difficult to estimate how many people around the world would like to have access to the Internet but do not have a service available, and when a service is available it is not affordable. Few countries publish information about Internet services so the number of people around the world who would like affordable access to the Internet cannot be calculated, however the number is likely to be in the billions. The characteristics of these potential WISP customers are listed below.

- Limited economic ability means the WISP has to provide a slower speed low cost rate plan, maybe $2/month for a 2Mb/s or $1/month for a 1Mb/s maximum download speed.
- The big proportion of prospective WISP customers do not have bank accounts or credit cards but does have cash to pay for the Internet service.

- The larger proportion of prospective WISP customers will seek a mobile broadband service, and access that service using a low cost mobile phone.
- A smaller proportion of the WISP's prospective customers will purchase a CPE installation for a fixed broadband service due to higher cost.

Many of the WISP's that the author has worked with are located in Central and South America, the Caribbean, countries in Africa and countries in Asia. The principal characteristics of WISP's in these areas are limited investment capability, and limited technical knowledge, but they have excesses of enthusiasm, energy and dedication, which are the main ingredients to be successful. While people with a strong technical background have many options to design, build and operate WISP networks, it is not easy for the entrepreneur with limited technical knowledge to start a WISP business. This situation has improved recently with the availability of plug-and-play WISP management systems for people with limited technical knowledge. The author has been involved with the design of easy-to-use products for WISP's over many years, and this includes the easyWISP business management software described in this chapter.

9.2. The WISP business technical architecture

Most WISP businesses follow a similar design plan with technical infrastructure, dividing the network design into several elements. The first element is a tower with one or more PtMP wireless access points installed, and located at a high point in the terrain so that it is visible to the maximum number of potential subscribers. Depending on the speed of the Internet backhaul link and the performance of the wireless products, the tower may be able to provide an Internet service for between 50 and 300 subscribers. Each subscriber has a CPE wireless antenna installed at a high point on the building with a line-of-sight to the PtMP antenna on the tower. The second important element is the network operations center (NOC), which has the wholesale data connection to the Internet. The data circuit may be fiber or copper, or else the NOC might have a wireless point-to-point connection to the wholesale Internet service provider. Finally there is a point-to-point wireless connection infrastructure between the tower and the NOC.

The WISP business grows by adding a second then a third tower, and all towers have a PtP wireless link back to the NOC. In parallel the WISP contracts with the wholesale data circuit provider to increase the circuit capacity. As towers are built further away from the NOC then a single PtP link may not be possible due to the distance or due to obstacles in the path and so the tower is connected to the NOC with an intermediate wireless relay, so the PtP that has two 'hops'. A wireless PtP link can have several 'hops' however there is a practical limit as each hop will increase the latency or delay of the PtP connection.

The WISP will encounter logistical issues when constructing towers due to land leases and construction permits as well as locating NOC premises where the wholesale data circuits can be installed and also be able to install PtP antennas that connect to each tower.

The following figures illustrate the WISP's network as it starts with one tower then grows in size as PtMP towers are added so that Internet service can be offered to more customers.

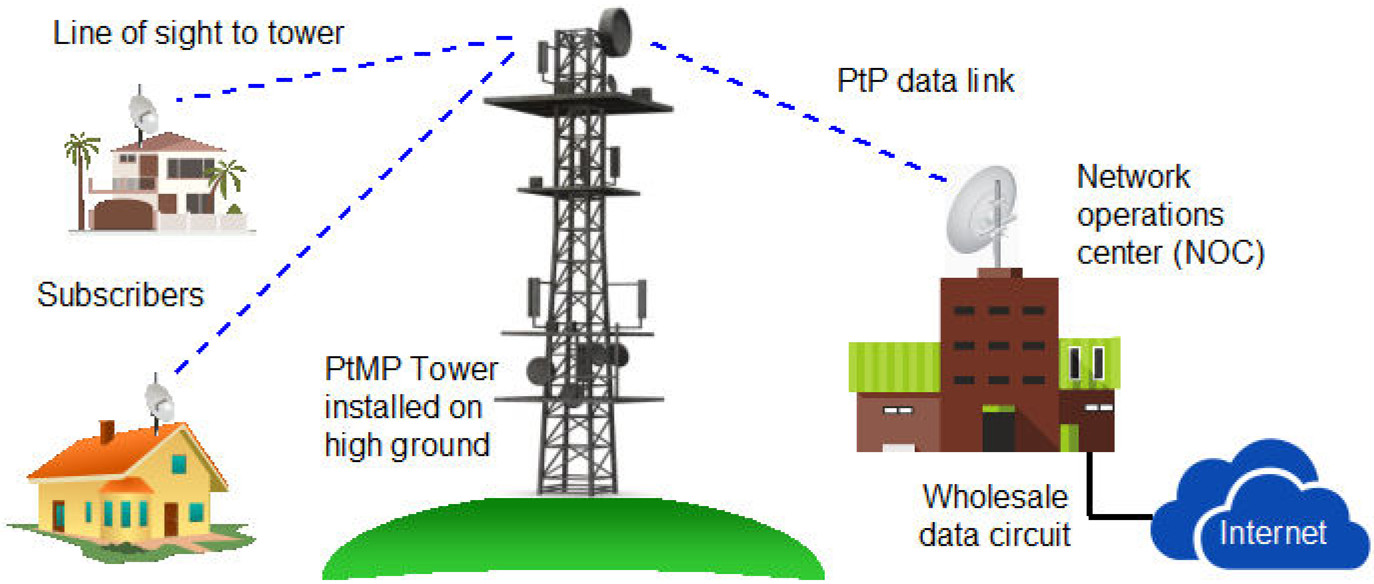


Figure 9.2.1. The WISP business basic physical infrastructure.

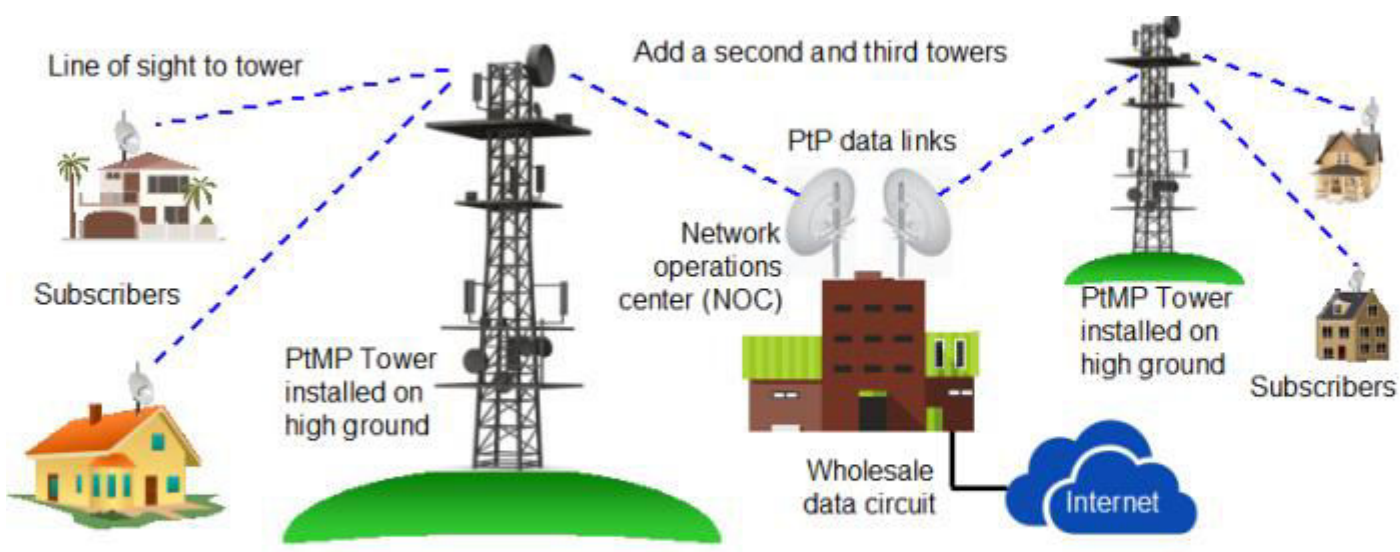


Figure 9.2.2. Expanding WISP business basic physical infrastructure to add subscribers.

The WISP has to design and build a computer network with the functionality to deliver a reliable Internet service and charge customers for the use of that service. Business functionality has been described in an earlier chapter however it is instructive to review the functionality again as part of the WISP's business startup process.

The WISP will install an access control router in the network path between the customers and the wholesale provider. The router has three tasks, listed below.

- Authenticate the customer onto the network using one of the methods previously described to verify that a legitimate customer is making the access, and prevent any fraudulent attempt to access the network.
- Apply the customers chosen rate plan, maximum download and upload data speed, and an optional data cap.
- Enable or disable the customer according to the status of the customer's payment regarding invoices issued.

The next diagram illustrates the WISP business functionality.

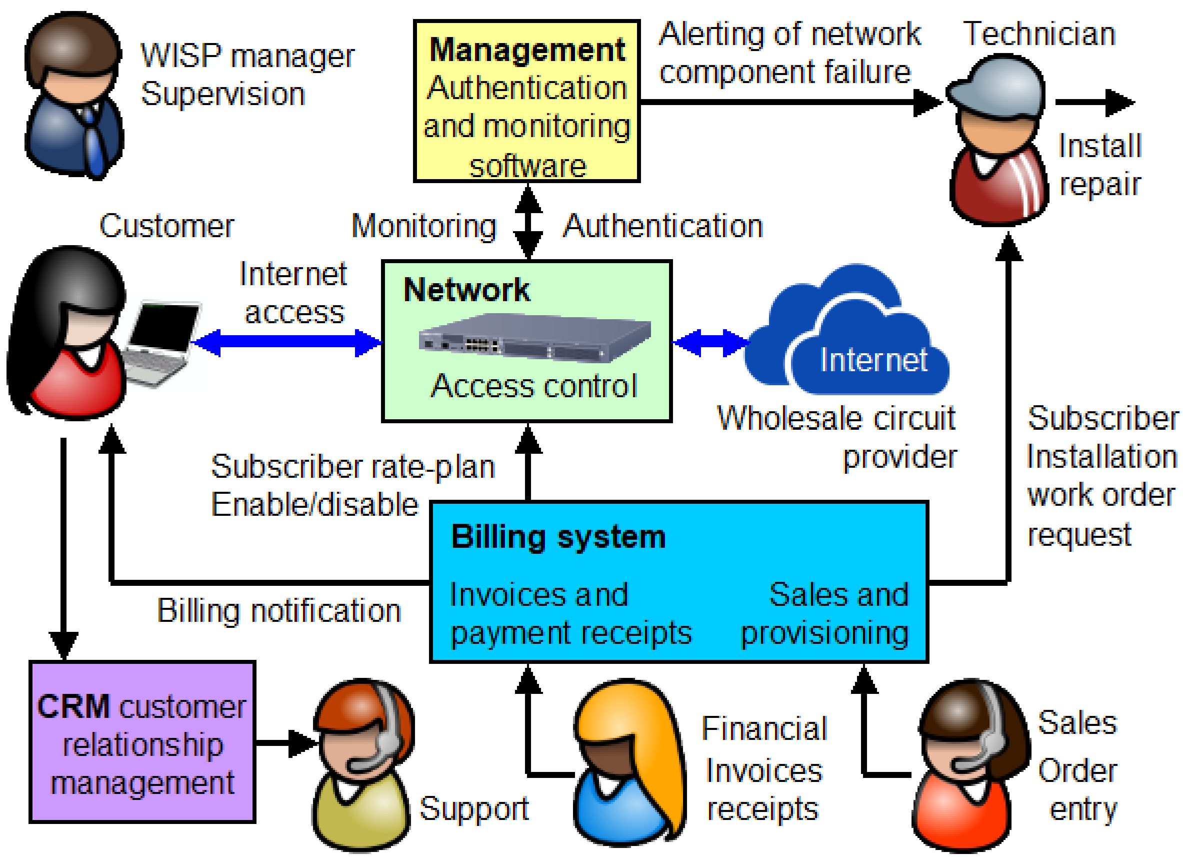


Figure 9.2.3. The WISP business automation functionality.

The WISP manager has a choice when designing the network, learn router programming and manage the process manually, or choose billing management software or cloud service that includes RADIUS authentication and access control programming. The router is configured manually using the command line interface or a router GUI if available. Alternatively the WISP can install billing management software that will configure the router via the router API interface with each customer rate plan and enable or disable each customer. The authentication process can be simple by adding the customer CPE MAC address to the router table, or more secure using a PPPoE credential entered at the CPE and verified at the router PPPoE server via an external RADIUS server. Authentication can also use WPA2-enterprise in which case the PtMP wireless will communicate with the RADIUS server to authenticate the credential that it receives from the customer CPE wireless. The RADIUS database will be programmed with the list of subscriber authentication credentials. Several cloud-based WISP billing systems also include a RADIUS server authentication service and synchronize the RADIUS database with the billing database for subscriber authentication, which simplifies the WISP technical management requirements. Software billing products that automate the router interface provide an initial script that has to be loaded into the router, and from that point on the software manages the router.

The startup WISP will Initially have the entrepreneur doing all tasks required to make the business operational with some help from specialist individuals. As the business grows then employees will be hired for specific roles within the business. There is a division of roles within the WISP business as follows.

- **Technical**: This includes network design, tower installation, NOC site installation, customer premises CPE installation, network equipment configuration, network repairs, and technical support.
- **Sales**: Advertising the services, speaking with potential customers, signing up subscribers, preparation of subscriber agreements, initiating the work order process for a new customer.
- **Financial**: Check the billing system daily and print the billing cycle invoices due to be sent out on that day, posting monthly invoices to subscribers, verifying if subscribers have made payments through the subscribers preferred method, recording the payments that were received in the billing system, maintaining the bookkeeping, ledger, accounts receivable, accounts payable, and staff payroll.
- **Customer support**: Customers and prospective customers will have questions about the service and so a member of staff is designated to answer questions, which may come via phone, personal contact or via the CRM system.
- **Manager**: Supervision of technical network design and operations, permitting and licenses, purchasing of materials for network expansion and customer premises installations, monitoring cash flow and tax payments, analysis to reduce costs and increase customer satisfaction, follow up with customer issues, follow up with sales and marketing results, negotiate with trunk circuit providers, set expectations for goals given to staff, and staff training.

The last element of the business model is a decision about what services will be offered and how the services will be charged. Services and payment plans that can be offered are listed below.

- Fixed broadband, charged by monthly subscription, can be pre-pay or post-pay.
- Fixed broadband, charged on-demand, always pre-pay.
- Mobile broadband, charged on-demand, always pre-pay.
- Mobile broadband, charged by monthly subscription, always pre-pay.

The WISP must make a decision about the rate-plan charges for the Internet service. Options are listed below.

- Monthly subscriber rate plans, data speed, data cap and charges (the subscriber is always connected unless payment is not received).
- Mobile broadband on-demand charges, connection duration, data speed, data cap and charges.

Payment of services for monthly fixed broadband subscriptions is usually pre-pay and depends on the payment methods available in the country where the WISP is installing the service. The WISP can issue an invoice to the customer requesting payment, and payment can be made by various methods including the following.

- Direct debit of a bank account.
- Payment billed by the WISP of a credit card provided by the customer.
- Payment on-line using a credit card.
- Payment via a check.
- Payment by cash at a WISP retail location.
- Payment by cash using a payment service (e.g. Oxxopay in Mexico).

Payment of services for on-demand mobile broadband is always pre-paid and is most often made by purchasing an access code, which is entered into a captive portal login page. Some people have set up a very simple service where the customer's device MAC is entered into the wireless access point allowed MAC table manually and removed manually at the end of the access duration. Purchase of an access code can be made by one of the following methods.

- Purchase an access code online via the captive portal login page using a credit card.
- Purchase of a voucher with the access code for a cash payment from the WISP's office or from an agent of the WISP.
- Purchase an access code from an agent of the WISP using a cash payment, the access code is presented on a mobile phone and noted by the customer.

The payment methods listed above are the most popular, however WISP's have created other payment methods that rely on a local cash payment service.

9.3. Locating the PtMP tower and the NOC

The first question that the WISP must ask when surveying a location to install the WISP business is the availability of a high bandwidth Internet circuit. If there is no local telecom company that can provide a circuit then the project cannot begin. At some time in the future the WISP will not have to ask this question because a LEO satellite service will be available and so a WISP business can be located anywhere.

The area where the wireless Internet service will be provided determines the location of the PtMP tower and the NOC. The PtMP tower should be located at a high point of the terrain overlooking the town. This will depend on the terrain and the availability of a lease from the landowner to install the tower. If the terrain is flat then the tower must be tall so that all residents have a line-of-sight to the tower. If a high terrain location is found then the tower can be shorter. As an alternative there may be a tall building in the town where the antenna can be installed. Suitable locations are church steeples or municipal water towers. If the PtMP tower is installed at a high point in the surrounding terrain there will be no power available for the tower equipment, and so power generation and storage using a solar panel with a wind turbine and battery will be installed at the tower. If the PtMP antenna is installed on a tall building in the town then power is likely to be available, however the WISP should install a power supply with battery storage for backup.

The photograph of a small town is shown in the next figure and illustrates an example of a WISP installation to provide the wireless Internet service.

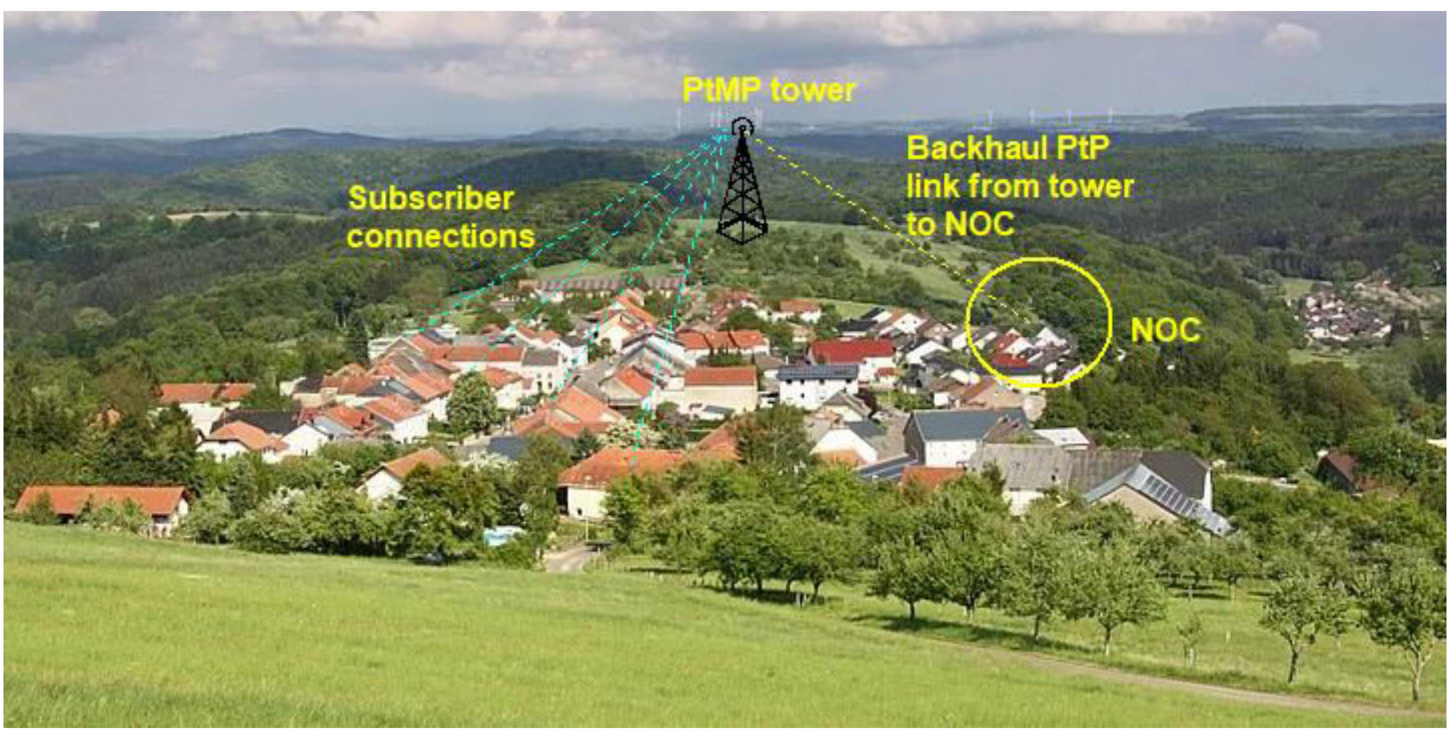


Figure 9.3.1. An example for the installation of the NOC and PtMP tower.

The NOC will be installed in a building that the WISP can lease and have the wholesale circuit installed. The type of circuit that the WISP can find will depend on the local telecom company who will provide the circuit. In the best case the WISP can get a Gbit fiber circuit installed. In the worst case the WISP may have to install several copper DSL circuits and connect to a load balance router to provide the bandwidth for the WISP services. The NOC connects to the PtMP tower via the PtP wireless backhaul.

9.4. A startup WISP network design

An important design decision regarding the network design is the location of the access control router in the WISP's network. The network design presented in this chapter proposes to install a smaller access control router at each tower, which is a departure from the conventional WISP network design of installing one access control router at the NOC. The reasons for this decision are listed below.

- The PtMP wireless access point can be installed at a location where there is Internet access, a mobile phone tower or tall building. If the access control router is not installed at the tower site then the PtMP wireless has to be connected back to the NOC access control using a VPN router, this will require an increase of the capacity and cost of the NOC trunk circuit and increase the circuit latency for the customer.
- The PtMP tower can be backhauled to any location that has a wholesale service, which might be much closer than a multi-hop PtP link back to the NOC. This will facilitate the WISP's network expansion as the WISP can install a number of smaller NOC's, each with a smaller capacity Internet trunk circuit that are conveniently located for a number of towers grouped around it. Reducing the number of backhaul hops will reduce the latency for the customer and provide a better quality of service.
- The PtMP tower can be upgraded to a LEO satellite backhaul when the service becomes available, and new towers can be installed with a LEO satellite antenna to eliminate the installation cost of PtP backhaul links. This will reduce investment costs for the WISP and permit the WISP to increase the speed of expansion of the network to capture more subscribers.

The disadvantage that some WISP's may observe with this network design is that the WISP has to login to multiple routers to enter the customer access control parameters as towers are added to the network, rather than logging in to only one access control router at the NOC. This configuration requires that the WISP keep a subscriber record that includes the tower to which the customer is connected for configuration purposes.

A number of WISP cloud management systems with router automation via API's already support multiple access control routers as a router or tower is assigned to the customer together with the rate plan when the new subscriber information is entered in the WISP management system. From that point on the tower access control router is programmed by the WISP management system with the subscribers account information.

Several authentication methods have been described previously. The simplest method will be used in this design, which is CPE MAC address recognition. Both PPPoE and WPA2-enterprise require the installation and configuration of a RADIUS server and PPPoE requires the configuration of the PPPoE service in the access control router. Some WISP cloud management systems do provide a RADIUS server service and can program the PPPoE service in the access control router, or else the PtMP wireless has a WPA2-enterprise configuration to access the cloud service RADIUS server. When the cloud service includes a RADIUS server then the RADIUS server database customer credential will be updated from the billing system database so the WISP has no configuration for the subscriber credentials that are entered into the CPE wireless at installation.

The NOC is located in a building that has the characteristics listed below.

- A telecom company or wholesale Internet service provider can install a high-speed Internet circuit or circuits at that location.
- The location had line-of-sight access to the tower for the point-to-point backhaul link between the tower and the NOC.

The next figure is a schematic diagram showing the interconnection of components in the WISP network. The tower site has the PtMP wireless access point, the access control router and the PtP wireless backhaul installed. The tower also has sun and wind power generation and storage when necessary. The NOC has the wireless backhaul, a multi-WAN load balance router and the WISP management software. The WISP manager and staff are located at the NOC.

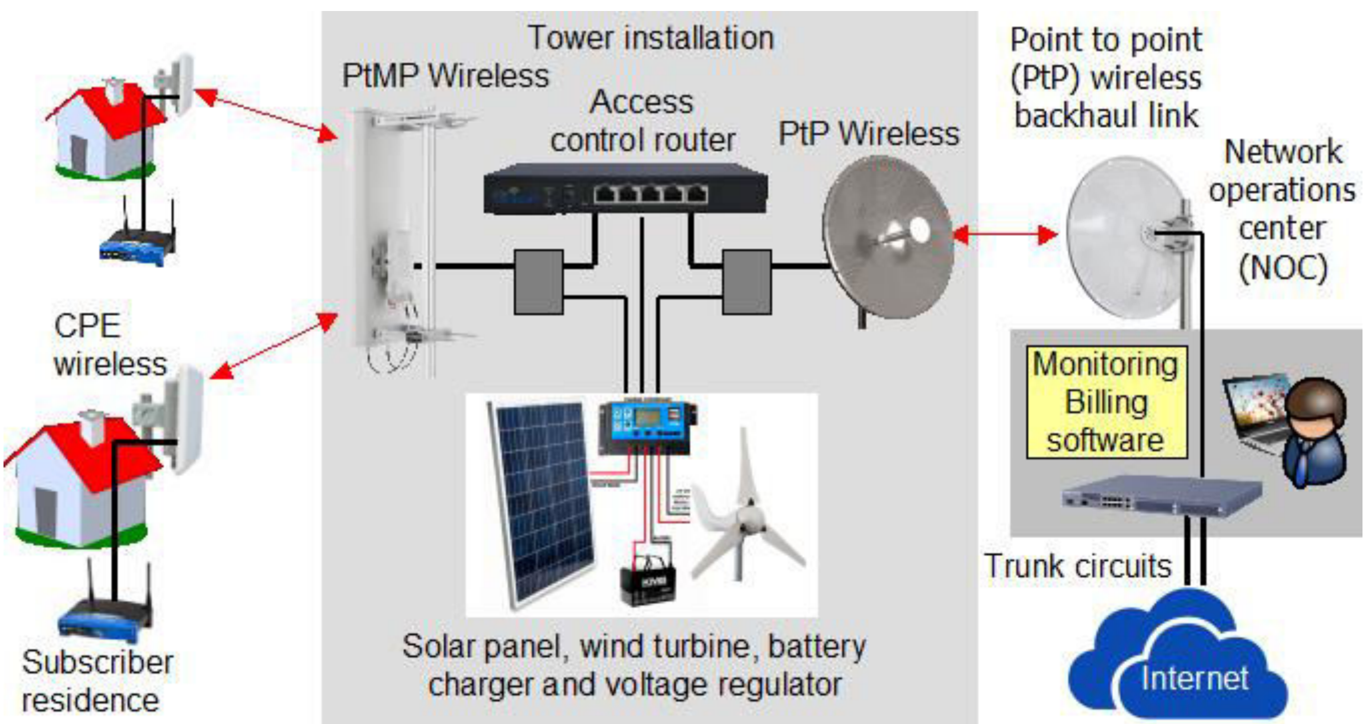


Figure 9.4.1. Basic infrastructure installation for the start-up WISP network.

9.5. Transitioning the WISP network design to LEO satellites at a later date

With the Internet connection technology available today, the WISP can only install a business where there is access to a fiber or copper Internet wholesale connection, or else use a bandwidth limited geo-stationary satellite service in one of the areas covered by the satellite antennas. Very soon a WISP will be able to install a PtMP tower anywhere on the planet with a high bandwidth LEO satellite backhaul connection. The WISP's network infrastructure will be simplified, as listed below.

- The NOC and the wireless distribution network infrastructure between the NOC and each tower is eliminated which eliminates a single point of failure and reduces the investment.
- The WISP installs management software in a cloud service such as AWS, or else contracts with a cloud service provider for a network monitoring, subscriber billing and router management service.

The following diagram illustrates what a WISP network schematic will look like when using the Starlink network to backhaul to the Internet. Each PtMP tower has an access control router and a Starlink antenna. The access control router is managed manually via the Internet, or uses automated management via cloud software.

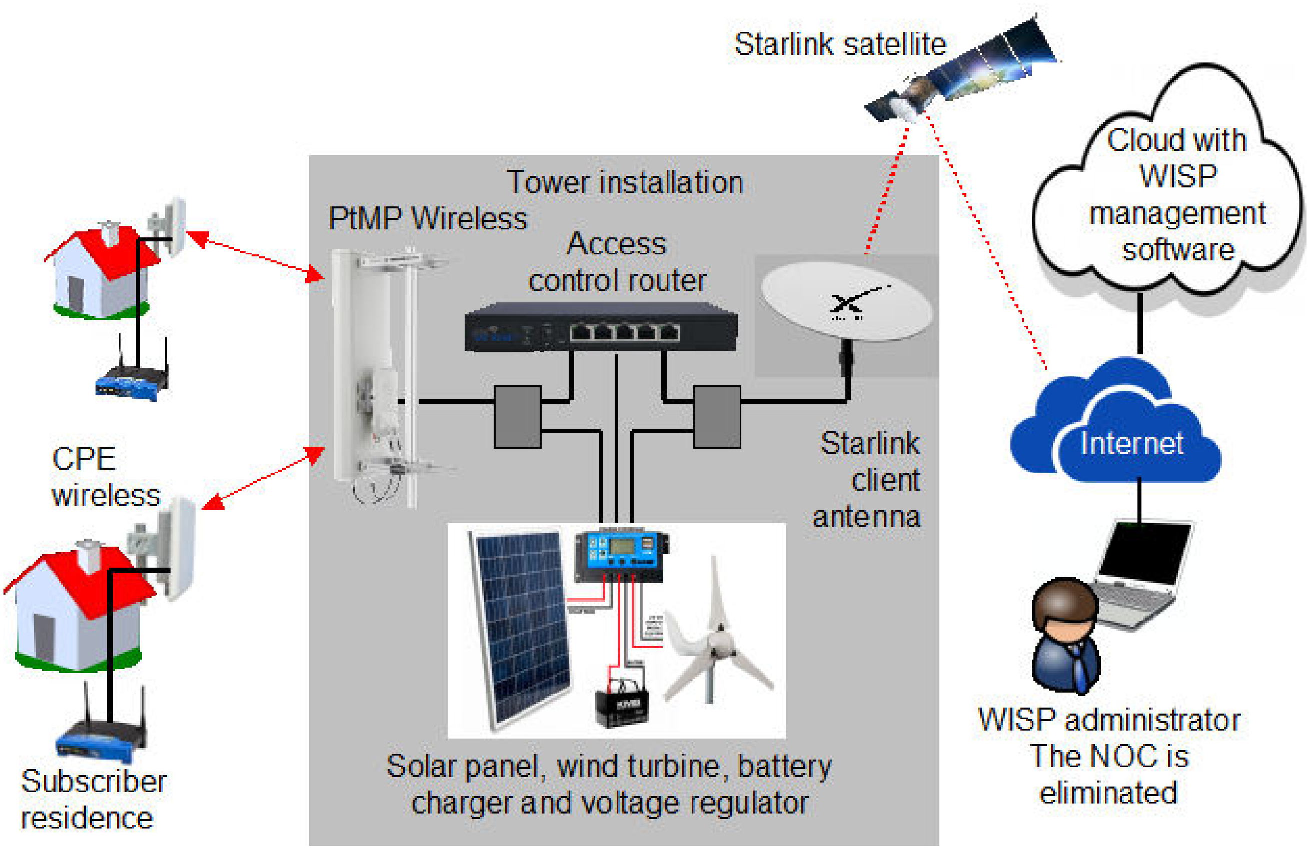


Figure 9.5.1. WISP network schematic with Starlink backhaul antenna and cloud WISP management. The NOC and PtP backhaul link are eliminated.

Many WISPs' are waiting for the availability of LEO satellite services like the Starlink service so that they can expand their networks outside the boundaries of their current areas of coverage. Some WISP's will loose customers who can afford to purchase a Starlink antenna and can pay for the monthly subscription. There are millions of people however who have no Internet service and cannot afford to pay for the Starlink service. The WISP's can use the Starlink backhaul to provide an Internet service for several tens of customers connected to each Starlink antenna, and provide the Internet service at an affordable cost. WISP's are likely to have an explosion of business as the USA has 14.5M rural Americans who don't have access to the Internet and need an affordable service. Around the world the number of possible WISP customers may reach 2 billion.

The WISP will have several options when LEO satellite services become available.

- Add a LEO antenna to existing towers and reconfigure the access control router to a 2-WAN-port load balance configuration to use both the NOC and the LEO satellite as backhaul links. This will increase the tower throughput permitting more subscribers to be added to the tower and provide redundancy in the case that one of the backhaul links fails.
- Switch an existing tower to LEO satellite only and eliminate the wireless distribution network and NOC to reduce operating costs.
- Build new towers with LEO backhaul only to reduce the installation costs as no PtP backhaul link is required, and permitting the towers to be installed at any location without regard to connecting the tower back to the NOC.

By installing the access control router at the tower for the network design recommended here the WISP is ready to migrate to a LEO satellite service when one becomes available.

9.6. Choosing the WISP administration software

The WISP has several choices for the management software that will help the manager and staff to administrate the WISP business. A comprehensive list of management software and cloud service providers is included in the Appendix. Management software ranges from free but with limited features and requiring extensive technical skills, to extremely comprehensive features and with plug and plan capabilities, but with a high operational cost.

Some examples of free WISP management software are listed below.

- Freeside is an open-source billing, CRM, trouble ticketing, network monitoring and provisioning automation software for ISPs and WISPs. The software is free to use and can be installed by anyone with Linux experience, however the company does offer charged installation and support services for users who do not have the technical experience required. The product has an on-line manual with full documentation. The product does not have a router interface and configuration of the access control router is manual.

- OpenWISP is an open source and free to use server plus client software that is used to manage and monitor any wireless or router product that has openWRT software installed. There are many openWRT products for networking that cost much less than comparable products from manufacturers such as Ubiquiti. A WISP manager who has good Linux skills and programming knowledge can therefore build a network with low cost openWRT based wireless products and routers by combining OpenWISP management software with Freeside open source billing software for a minimum cost network installation with no on-going charges for the use of a WISP management product.
- Ubiquiti UISP software is free and the company states that the product has network management, customer billing and CRM, but Ubiquiti does not publish specifications or a user manual so the only way to discover what features the product has is install it and test it. Ubiquiti has no support but questions about the product can also be sent to other Ubiquiti customers via the Ubiquiti user group. There will be a cost to host this software, either on a local server with power backup, or a remote server such as AWS. There is no charge per subscriber and no limit to the number of subscribers. The software is installed on a Linux platform and the Linux systems supported include Ubuntu. A WISP who installs this software must be familiar with Linux command line instructions and must have a familiarity with Ubuntu. The product does not have an access control router interface therefore the configuration of the access control router is manual. Ubiquiti offers a free hosting service providing that the WISP purchases 10 or more Ubiquiti Air products and so the software appears to be a tool to push product sales.

Some examples of WISP cloud management tools are listed below.

- VISP is a very comprehensive WISP billing and network management cloud service and also includes a cloud based RADIUS server for customer authentication where the RADIUS authentication database is synchronized with the billing database. The cloud service is plug and play and has an API interface with the range of Mikrotik routers that are used to implement access control. The VISP system is popular with WISP’s in the United States. There is a monthly charge to use this service, which is in the range of $1 to $2 per subscriber per month, depending on the volume of subscribers.
- Azotel is a WISP management service that is used by WISPs in the USA and other parts of the world. Azotel features include network monitoring and customer billing, and Azotel includes billing for both fixed broadband subscribers and mobile broadband on-demand customers. Azotel provides a plug and play solution with a dedicated server and access control router for NOC installation and access control routers for mobile broadband sites. The Azotel service also interfaces with Mikrotik routers. There is a monthly charge per subscriber for this service that is determined by the volume of subscribers.
- EasyWISP is a basic WISP management product service which has all the functions required to manage a WISP business, including monitoring of access controller failures and alerting, order entry with subscriber installation work order

and subscriber billing for both fixed and mobile broadband, customer relationship management portal with on-line payment facilities, and customer authentication using several methods. The software is plug and play and has an API interface to the easyWISP dedicated access control router and also for the range of Mikrotik routers. The cost of the easyWISP is the lowest of all WISP cloud management products and is in the range of 20 cents per subscriber per month. The product is multi-language and was designed for startup and growing WISPs in developing economies around the world. The author was a consultant for the design of the EasyWISP product.

The easyWISP software was selected to explain the installation and operation of a WISP. A diagram showing the system architecture of the easyWISP system is included below.

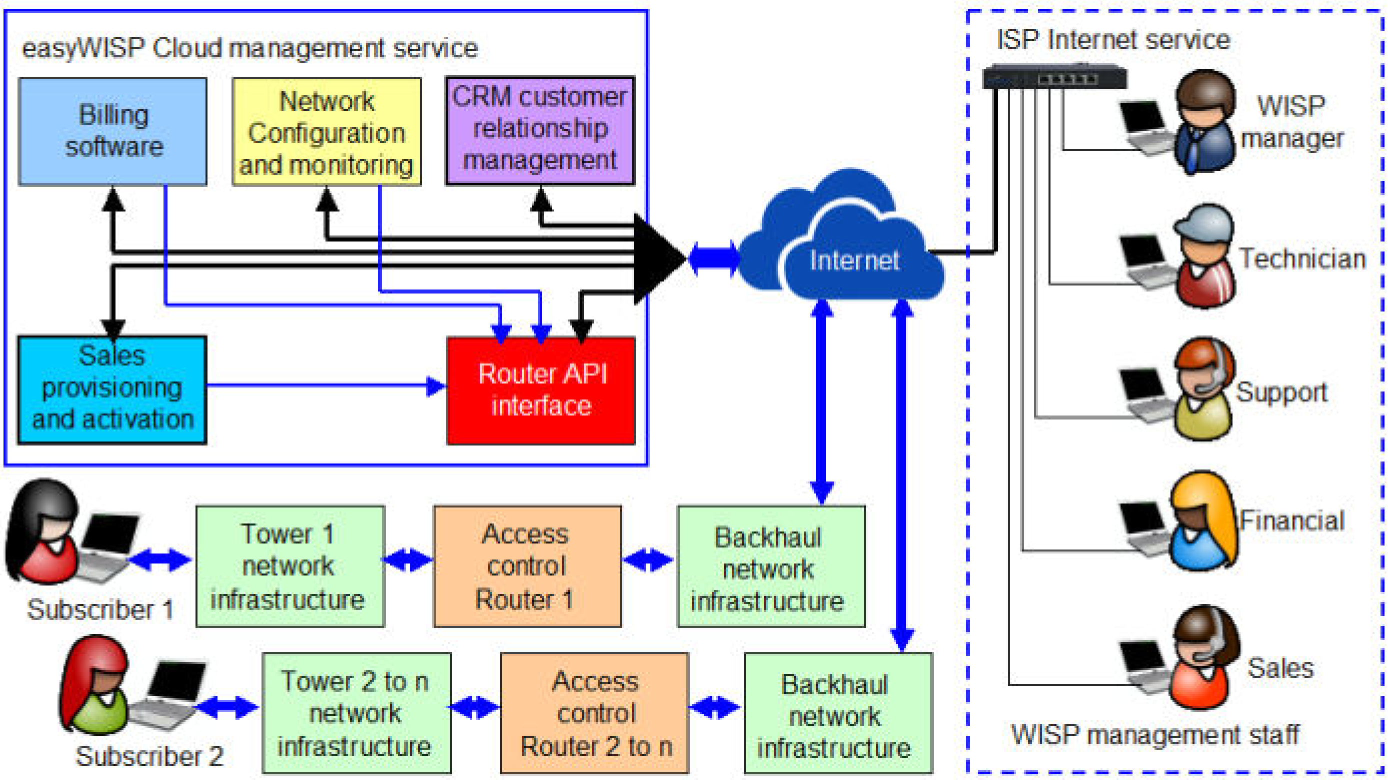


Figure 9.6.1. The easyWISP management system architecture.

The decision for the choice of WISP management software is based on six criteria.

- Cloud management is advantageous because it eliminates the need to set up local servers or set up a managed cloud service such as AWS, and requires far fewer technical skills to set up and use.

- Ease of use with plug and play access control router management is essential to eliminate the need to learn router-programming skills.
- The software product chosen must include all the features necessary for managing the WISP business.
- The software product must support the management of multiple routers so that access control can be installed at each tower, ready for future expansion.
- The software product must have a very low operating cost, as it will be used in parts of the world where the charge per customer is very low.
- The software product must function with any type of Internet backhaul, including a LEO satellite system.

The easyWISP system is used by WISP's in South and Central America and countries of the Caribbean and Africa where economic limitations do not permit the use of software products that have a higher cost of operation, or software products that require a high degree of technical knowledge to install and operate. Cloud for WISP has two limitations. The first is that there is no automatic process to issue customer invoices, the staff have to monitor the customer report daily and issue invoices on the date required. The second is that there is no SNMP monitoring for network products as the system uses a proprietary monitoring process for the access control routers; therefore an additional SNMP monitoring software is required.

The WISP manager first creates an account with the easyWISP cloud service using the first router. The router can be installed at the NOC or at the tower, and in this design the router is installed at the tower. There is no limit to the number of access control routers that can be added to the account, and no limit to the number of subscribers that can be added to the billing system. When a subscriber is added to the billing system the tower that will service the subscriber is added to the account.

The cloud4WSP system has five roles that are listed below, each with a login that restricts access to all parts of the cloud account. Multiple employees can be assigned to each role if required.

- **Manager**; access to all parts of the system, including reports.
- **Technician**; access to the network configuration, work orders and customer provisioning and failure alerting, inventory of access control routers and status of each.
- **Support**; access to customer information, circuit testing out to the customers CPE and the CRM customer support ticket system.
- **Financial**; access to the billing system, issue invoices, mark accounts as payment received.
- **Sales**; access to enter and edit customer information, select rate plans and issue an installation work order to technical staff.

Staffs do not have to be in one location to access the WISP's cloud account, and can login from any location that has Internet service.

As PtMP towers are added to the WISP's network an access control router is installed at the tower and added to the easyWISP account. From that point on all new subscribers who are serviced by that tower have the tower name included in the customer profile.

9.7. Choosing the access control router

Routers manufactured by Mikrotik are very popular and available worldwide in more than 150 countries. The products are also low cost and very robust. For this reason Mikrotik products are chosen by most WISPs for network routing and access control applications. However programming and using Mikrotik routers for access control requires a very high technical skill level.

The easyWISP access control router was designed as a very efficient router for use with easyWISP. The easyWISP router does not have conventional router features but was designed with software developed specifically for WISP access control applications. The easyWISP router is fully redundant as it downloads the subscriber database for the subscribers serviced by the tower or network where it is installed. If the easyWISP router looses contact with the easyWISP system it continues to function and ensure that all customers have Internet service.

The easyWISP access control router was chosen for this example because it is easy to install and has excellent performance. The only configuration that may need changing is the router WAN port that has a default of DHCP client. If the easyWISP controller is connected to a fiber modem then it can be configured with a static public IP address. The WAN configuration depends on the type of service that the router is connected to. Connect the easyWISP router as shown in the figure below to set the password and check the configuration.

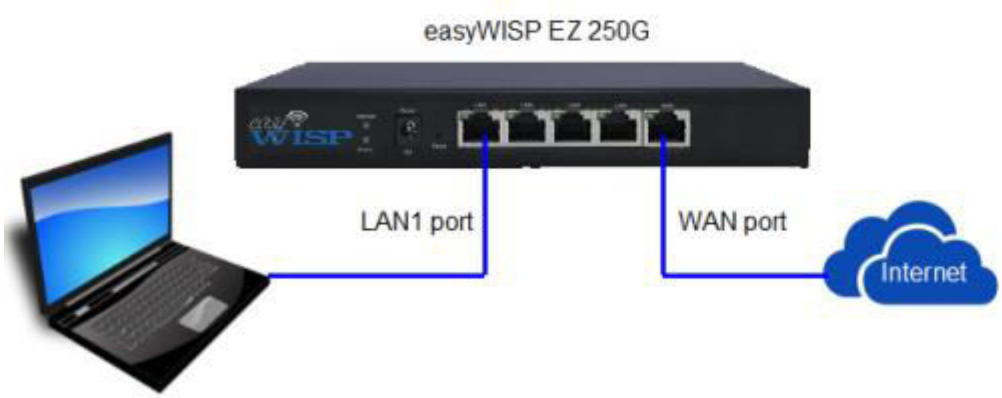


Figure 9.7.1. Connect a computer to configure the easyWISP access control router.

Open a browser tab and type 'wisplogin.com'. The screen shown in the next figure will be displayed. Make a note of the easyWISP device ID then set the password and make a note of that. Scroll down the page and check the WAN settings, if DHCP client is satisfactory then no change is required. If a static IP is required then set that in the space provided and click the update button. Scroll down further to see the firmware update box. EasyWISP firmware updates are always applied automatically however if the device has no Internet connection then the firmware update can be uploaded. The final window called network tools has several diagnostic tools that are available to test the WAN circuit in the case where the easyWISP shows that there is no Internet connection.

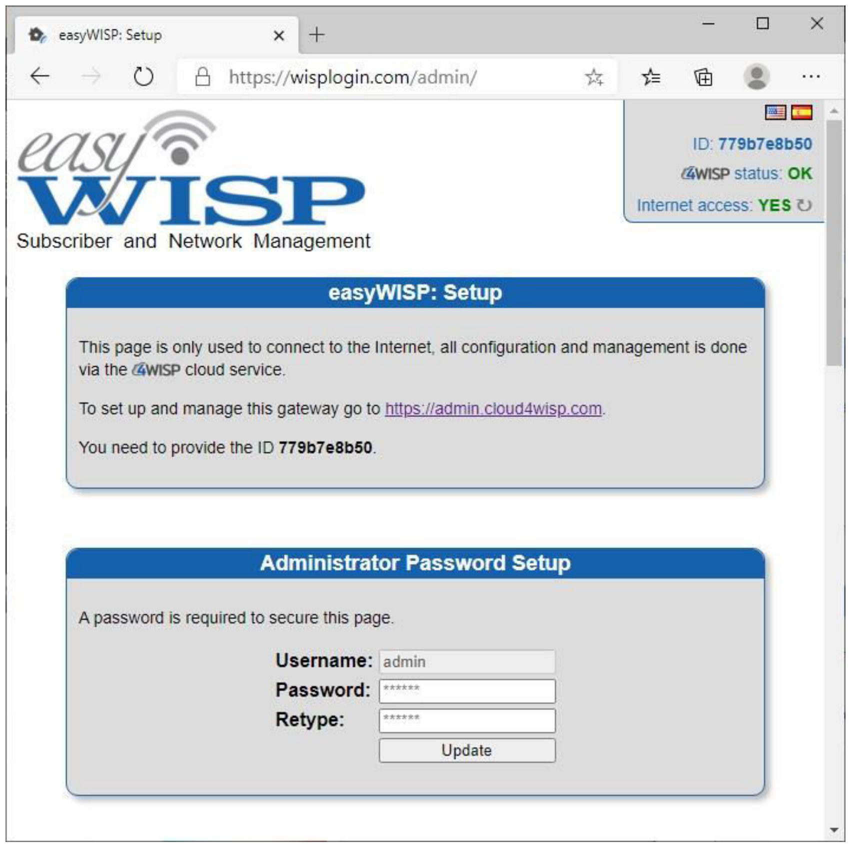


Figure 9.7.2. Open the browser tab to set the easyWISP password. Make a note of the password and the device ID, which is required for the easyWISP software.

Add the router license ID number to the easyWISP account. When the easyWISP access control router has been added to the easyWISP account then it will be programmed with the subscriber database by easyWISP and will then operate autonomously. The easyWISP router will send periodic updates to the easyWISP account with traffic and performance information. If the easyWISP operator makes any changes to a customer profile or adds a new customer for that router then easyWISP will update the easyWISP customer database.

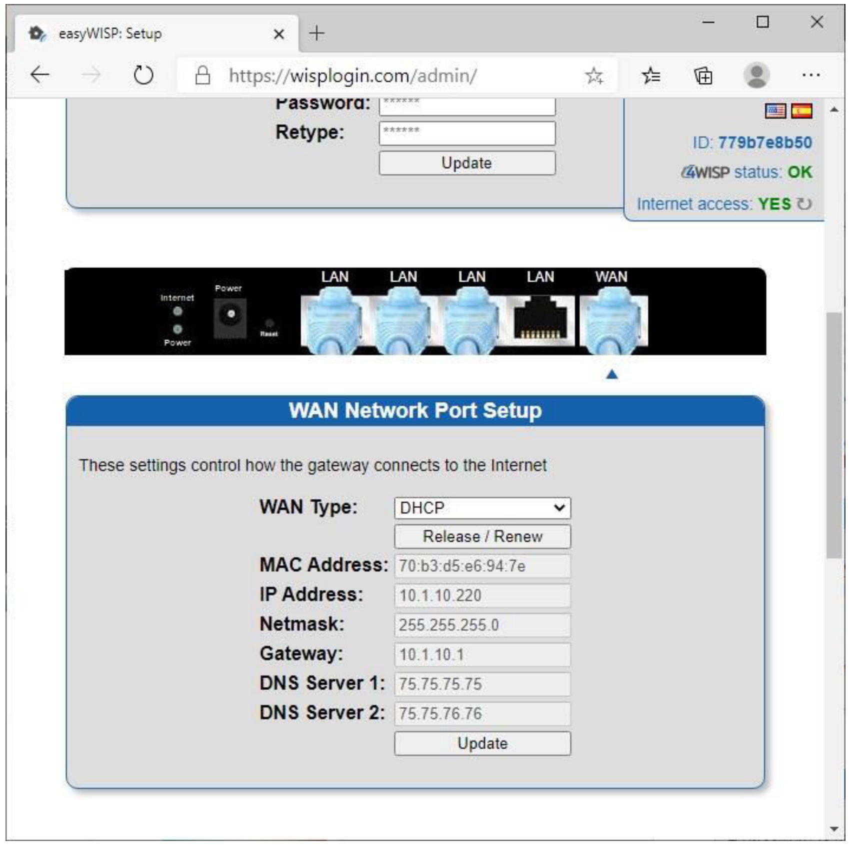


Figure 9.7.3. Scroll down the page to check the LAN port settings, verify if a DHCP client setting is correct or if a static IP is required.

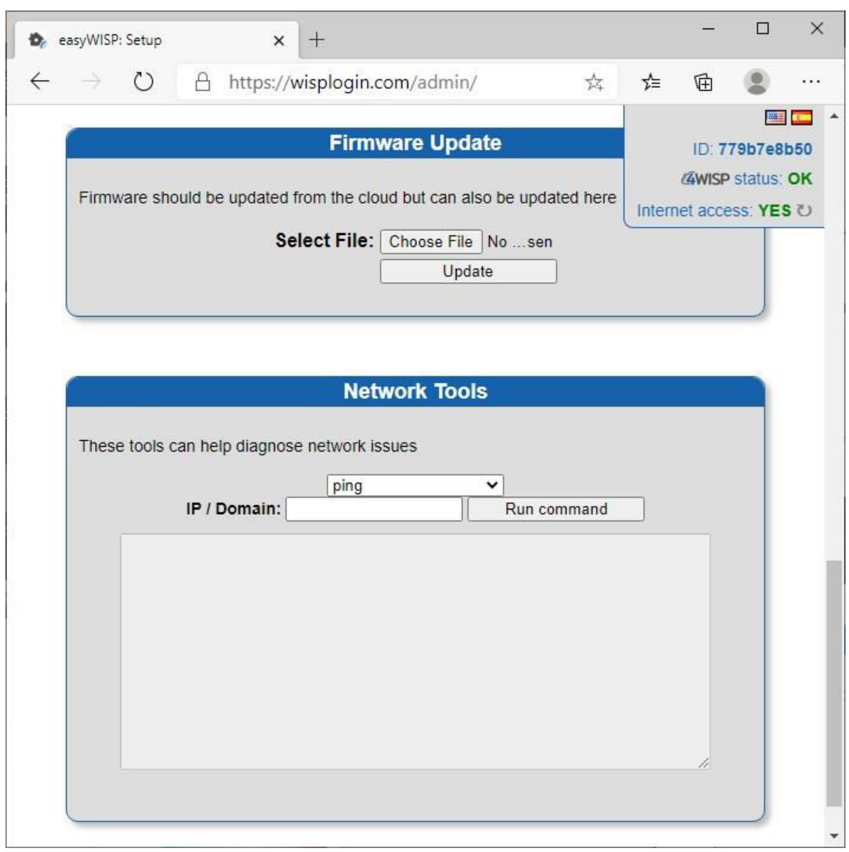


Figure 9.7.4. The easyWISP router firmware is updated automatically, however manual firmware installation is provided. The easyWISP also has diagnostic features for testing the circuit from the tower site.

9.8. Network build-out

The WISP network is built out in stages, where each stage is tested for functionality. The stages are sequential as follows.

- Build the network operations center (NOC), install and test.
- Install the first PtMP tower installation, test PtMP wireless.
- Configure the PtP wireless link between the tower and the NOC.
- Test Internet access via a CPE wireless.
- Begin selling customer installations.

The NOC design is simple as the access control functionality is installed at each tower and the management of the business operations uses the easyWISP service. A router is configured for a multi-WAN connection with load balance and fail-over. It is likely that the WISP have to contract with more than one wholesale provider to obtain the bandwidth required for multiple towers. The tower backhaul PtP antennas connect to the router. The staff computers connect through a switch to the Internet to access the easyWISP service. A power supply with battery backup is required to continue operations when a power outage occurs. The schematic for the NOC design is shown below.

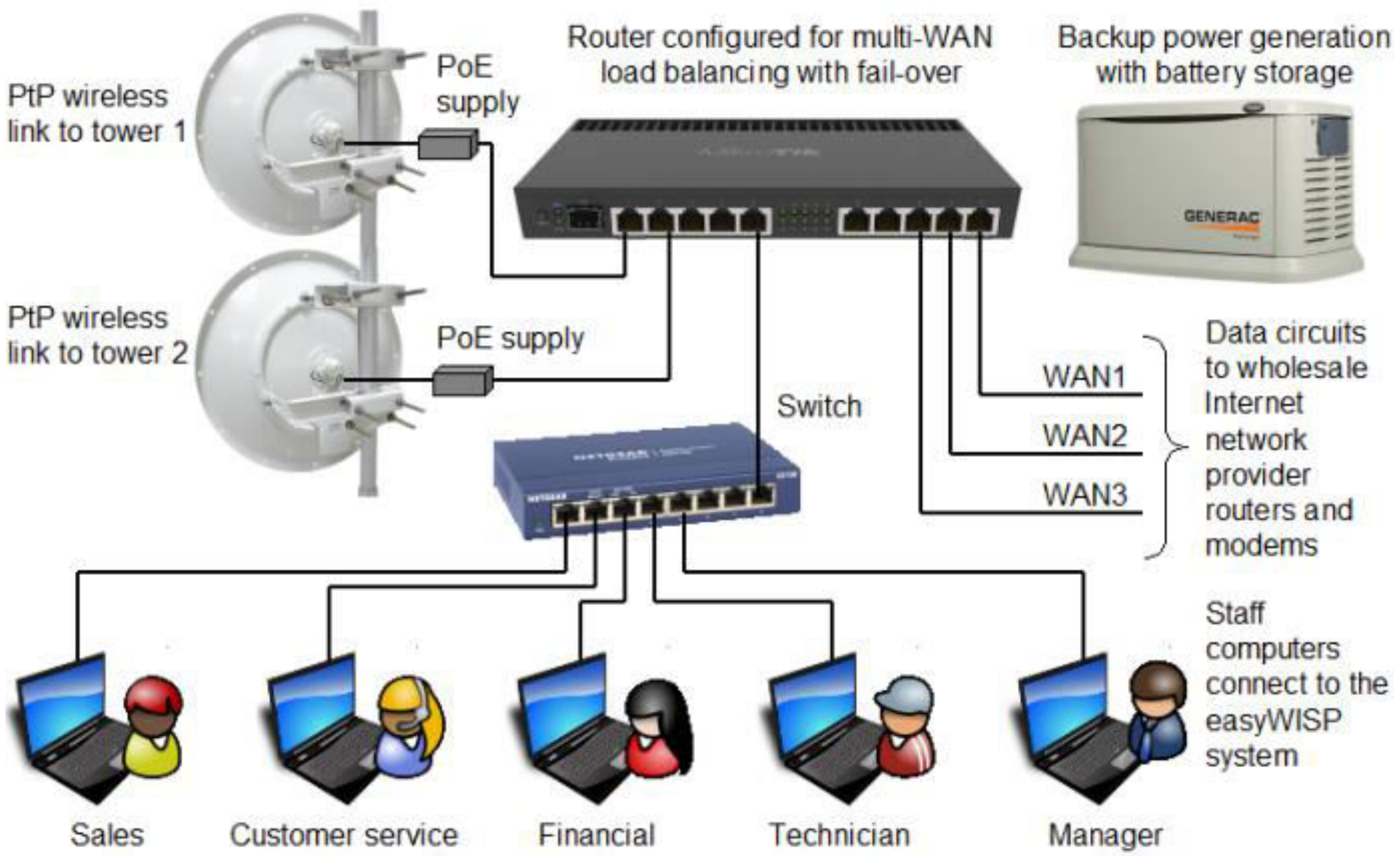


Figure 9.8.1. The network operations center (NOC) schematic.

The NOC has the following facilities for sales and technical staff in addition to the technical infrastructure.

- Sales: retail office to demonstrate the Internet service and to receive cash payments from customers.
- Technical: warehouse to store parts and equipment for customer premise installations and network maintenance.
- Technical: garage space for one or more trucks required to be rolled out for network maintenance and customer premise installations.
- Technical: workshop to test and configure equipment.

The tower site technical installation has three alternatives. First is a tower installation that requires power generation and PtP wireless backhaul. The second tower installation is a mobile phone tower that has power and an Internet connection with the capacity required for the subscribers who will connect to the PtP antenna. The third tower installation has a LEO (e.g. Starlink) backhaul antenna.

The new tower installation schematic shown in the following figure is recommended to use PtMP wireless access points with sector antennas as sector antennas are very efficient and low cost.

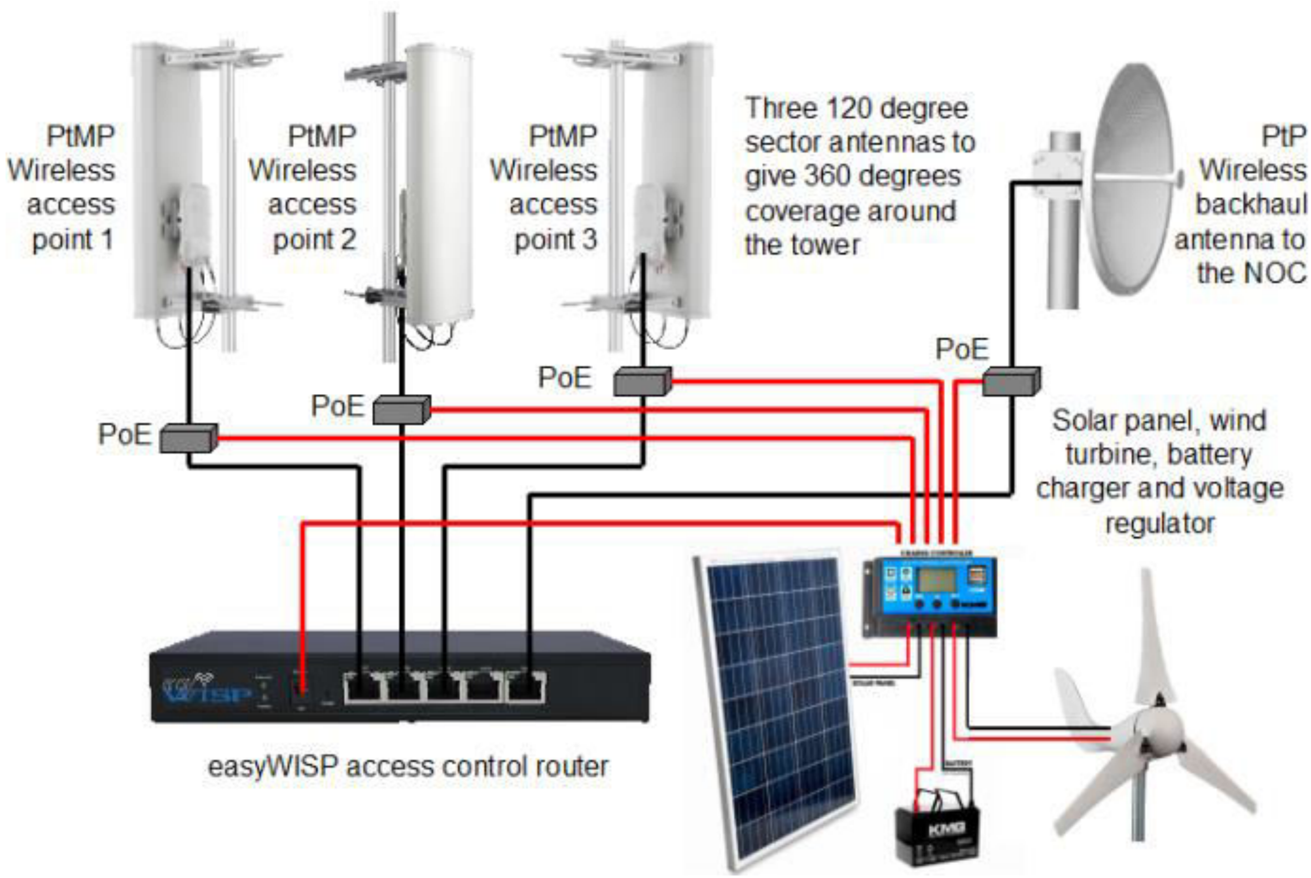


Figure 9.8.2. PtMP tower schematic for a new tower construction.

High power wireless access points with sector antennas can cost less than $100 in the USA. The most popular sector antenna provides radio frequency (RF) coverage over an arc of 120 degrees, with a vertical arc of 10 degrees or less. If the WISP wishes to provide RF coverage 360 degrees around the tower then three 120 degree sector PtMP access points are installed around the tower. In an installation where the tower is installed on a hill overlooking a town then one antenna with 120 degrees of arc may be sufficient. If multiple PtMP wireless access points are installed then each should be configured for a different wireless channel to minimize interference. Each PtMP access point is connected to a LAN port on the easyWISP access control router. The WAN port of the easyWISP access control router is connected to the PtP wireless antenna, which provides a backhaul connection to the NOC. Both the tower PtP backhaul and NOC PtP antenna will require careful alignment to get the best signal to noise ratio for the link with the highest data rate.

When the WISP is installing a network in a small town it is often possible to install the PtMP antenna on a water tower or a tower that was constructed for mobile phone antennas. Infrastructure service companies construct mobile phone towers then rent antenna space to several mobile telecom companies.

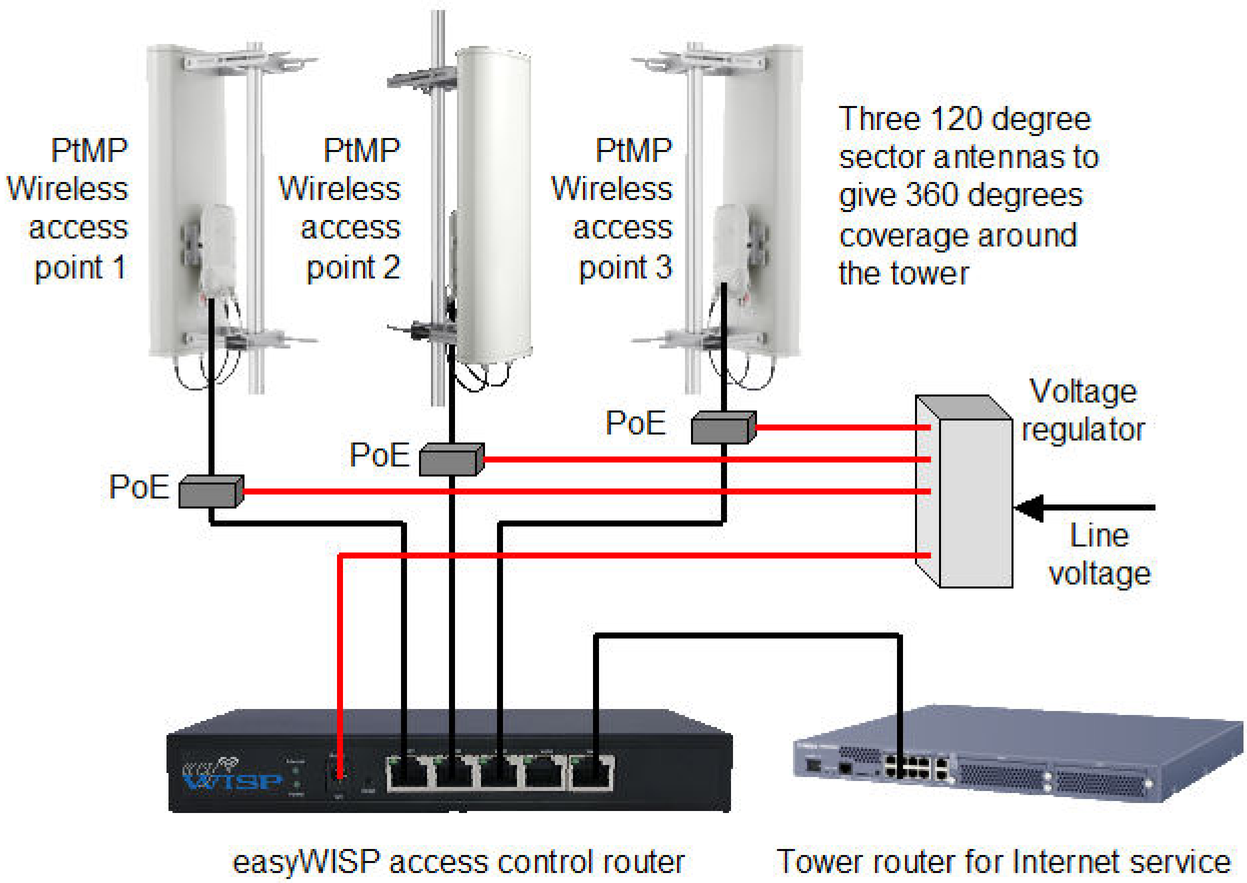


Figure 9.8.3. PtMP tower schematic, installation in a mobile phone tower.

The mobile phone tower has an electrical supply with backup battery storage, and has a high-speed network connection. The towers also have space to install equipment in a wiring cabinet at the base of the tower that is hermetically sealed and cooled. The rental cost of a mobile phone tower is higher than other types of towers however it is very convenient to install equipment so that the WISP can begin servicing customers very quickly. There will be an installation cost, as the WISP will have to pay the tower company to provide staff to install the antennas and equipment. One or more PtMP wireless access points are connected to the easyWISP access controller. Once again wireless access points with sector antennas are recommended. The WAN port of the easyWISP access controller is connected to the router provided by the tower company. The WISP will also install a power supply that regulates the line voltage of 110v down to the voltages required by the equipment.

When a LEO service is available in the WISP's area then new towers can be built with LEO antennas and existing towers can be converted to LEO antennas if required. The installation schematic is very similar to the tower with PtP backhaul. However the backhaul wireless antenna unit is replaced with the LEO antenna unit. One PoE supply powers both the Starlink antenna and the Starlink router.

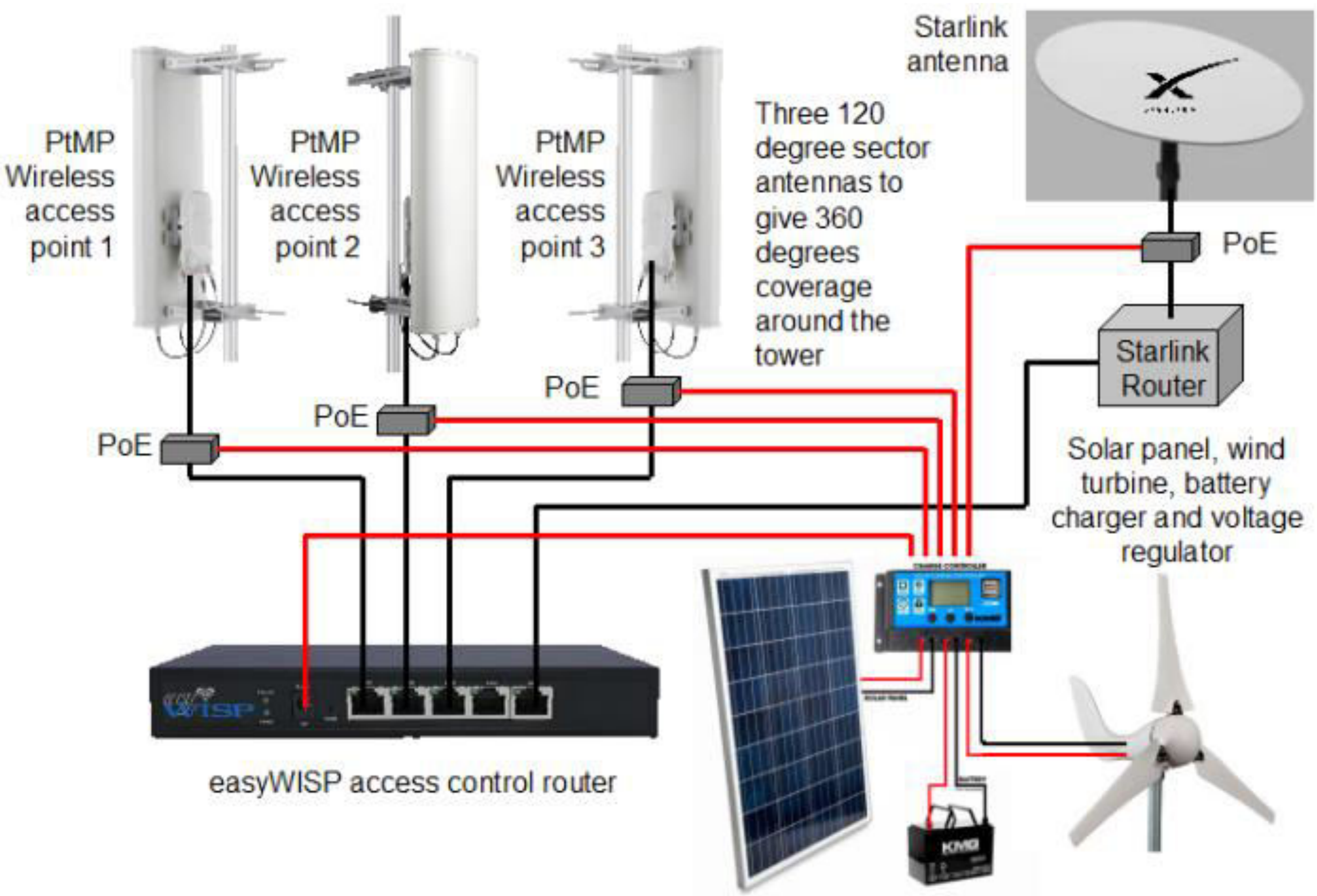
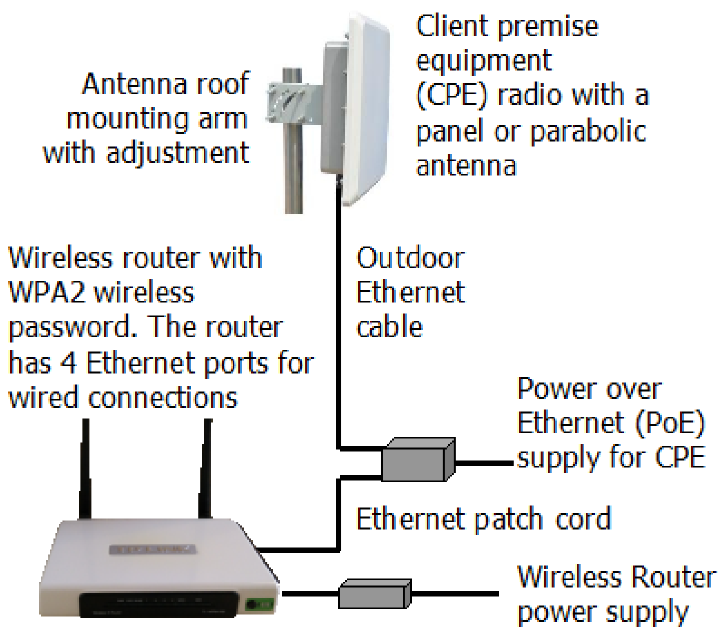


Figure 9.8.4. PtMP tower schematic for a new tower construction when the Starlink service becomes available.

The easyWISP WAN Port is connected to the LAN port of the Starlink router. Power generation and storage capacity should be increased considerably as the Starlink antenna consumes much more power than the PtP backhaul antenna.

Each fixed broadband customer premise installation has the same kit of parts; the only variables are the length of the Ethernet cable to the CPE wireless on the roof of the building and the location of the wireless router inside the building. The CPE antenna must be mounted on a high point of the building to have a clear line-of-sight connection with the PtMP tower. The installation technician must verify the line-of-sight connection before the installation commences. The wiring schematic for the customer premise installation is shown in the next figure. A PoE supply provides power for the CPE wireless and a second power supply provides power for the wireless router.

Figure 9.8.5. Customer premise installation schematic.



The installation procedure for the CPE requires the technician to first connect the CPE to a laptop computer to login to the CPE software. The technician selects the PtMP tower SSID and enters the key for the WPA2 encryption. The technician then opens the signal strength indicator and adjusts the direction of the antenna for maximum strength. The final step is to enter the authentication key if PPPoE is use for authentication. The technician sets a WPA2 key in the wireless router and connects the CPE to the wireless router WAN port. The technician can test the Internet connection by logging into the easyWISP system to activate the customer. The technician should request the customer to sign off that the installation is completed and is working satisfactorily.

When the network is operational with one tower and customers are using the service the WISP can plan network expansion. The next steps to build out the network are to add a second tower with backhaul to the NOC.

9.9. The WISP management system router interface

Many cloud implementations require the cloud service to call the local device in order to configure the device. This configuration requires port-forwarding rules in the routers of the local network. The easyWISP API interface for easyWISP routers does not require port forwarding in the local network. An installation with a backhaul via a mobile phone tower router or LEO network may not permit port forwarding for security reasons.

The design of the could4WISP system with easyWISP routers implements device polling of the cloud to request instructions. The easyWISP router periodically calls the easyWISP server to send traffic information to the server, or to request any instruction from the server. If the easyWISP server has any changes in status, such as a new customer added to the tower then the appropriate information is sent to the access control router when the router polls easyWISP. The next diagram illustrates the easyWISP interface with the easyWISP routers.

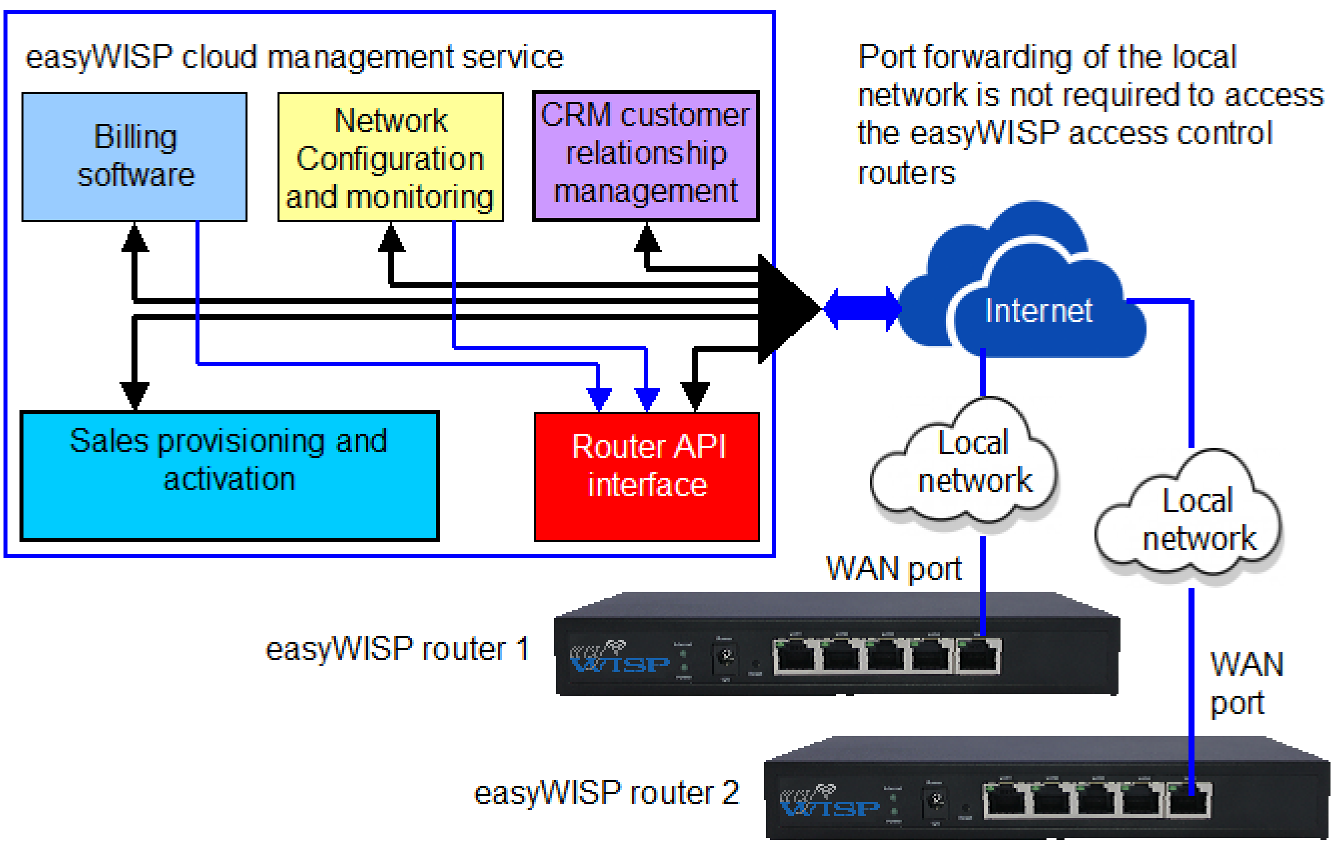


Figure 9.9.1. The access control routers communicate with easyWISP by polling the easyWISP service through the WAN Port API.

9.10. Create a easyWISP management account

Creating a new WISP account using easyWISP is a simple process. First open a browser tab using the URL.

https://admin.easyWISP.com/

The login screen is displayed. Select create new account.

Figure 9.10.1. easyWISP screen showing the account login screen.

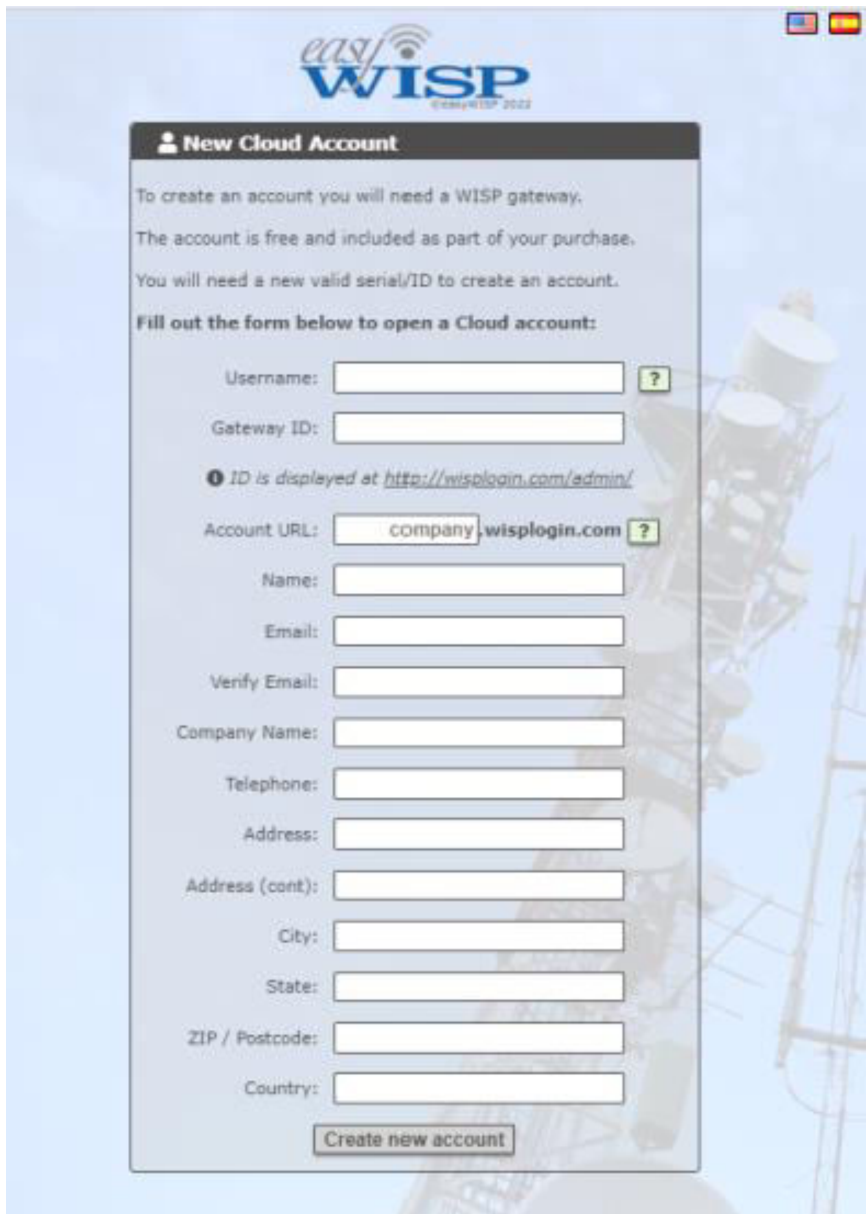


Figure 9.10.2. Add a username and the first router gateway ID then enter the WISP's account information. Finally click 'create new account' and an email will be sent with the password for the account.

After clicking the 'create new account' button the WISP will receive an email message with the login password.

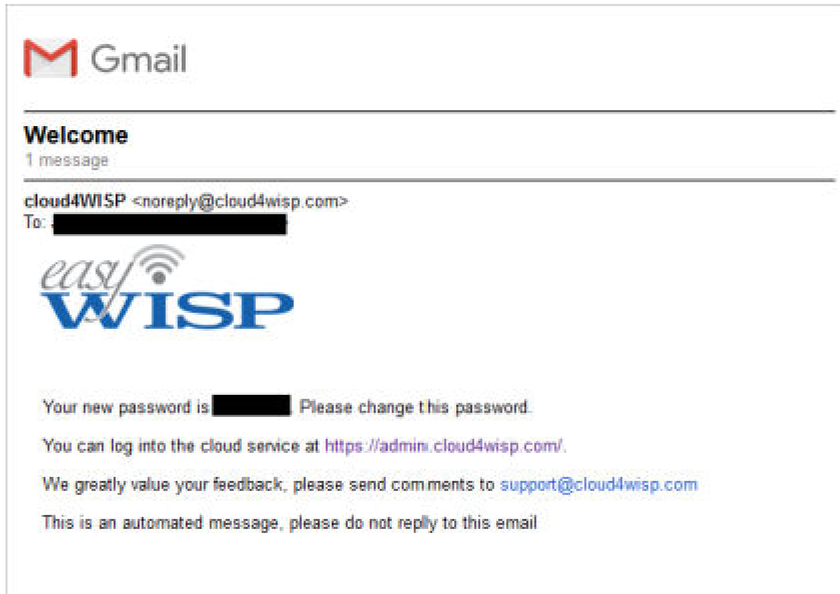


Figure 9.10.3. easyWISP welcome message with the account password.

Return to the login page to login with the username and password. On login the WISP will see the dashboard display. One router gateway will be shown, this is the router that was added when the account was created.

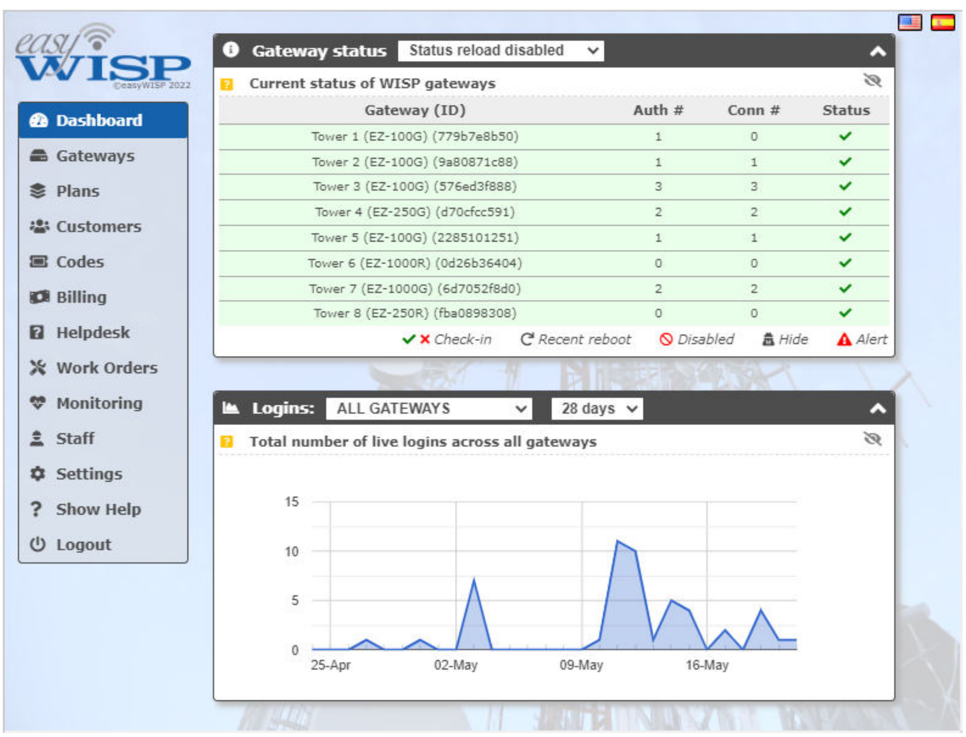


Figure 9.10.4. The dashboard display provides a summary of operations. The menu on the left of the screen selects the function required.

9.11. WISP management system initial setup

The first step after creating a new account is to configure parameters that prepare the account ready for use. The menu items that should be configured first are settings, staff and monitoring. The first step with new account is to click on settings to change the password from that provided in the welcome message.

Figure 9.11.1. Settings menu. Change the manager password.

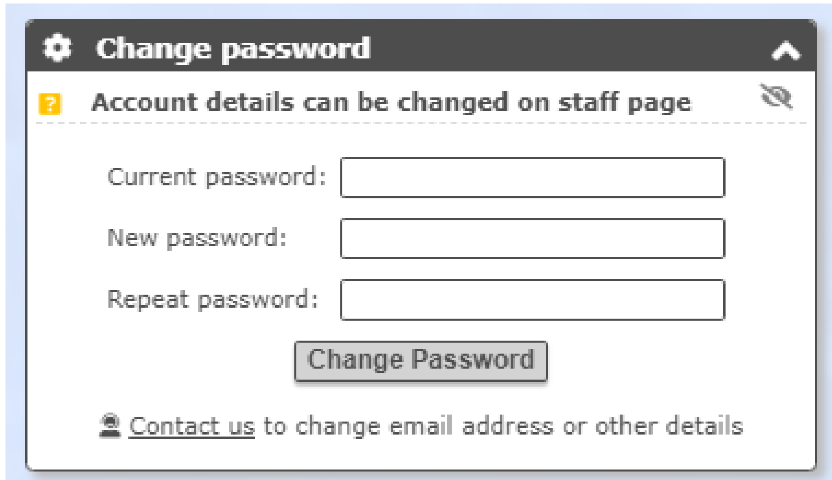
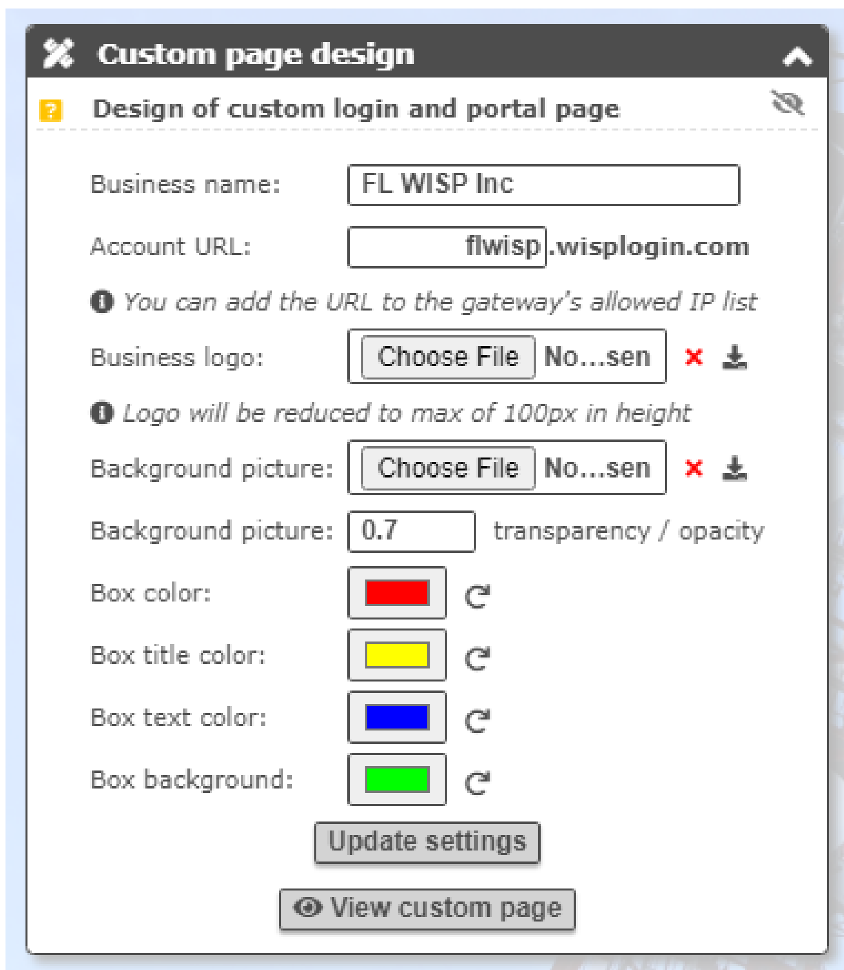


Figure 9.11.2. Settings menu. The captive portal design requires configuration.



The captive portal page is part of the Customer Relationship Management (CRM) interface and has a simple configuration process. The business name is entered for display on the page. A unique portal page is created using the WISP business name; this is the URL that WISP customers will use to access the CRM pages.

<business name>.wisplogin.com

The WISP can then upload a background picture or graphic, and the business logo. The WISP then chooses the transparency or opacity of the background and selects the colors of the login box. Finally the WISP clicks the update settings button to save the screen design. An example captive portal is shown in the figure below.

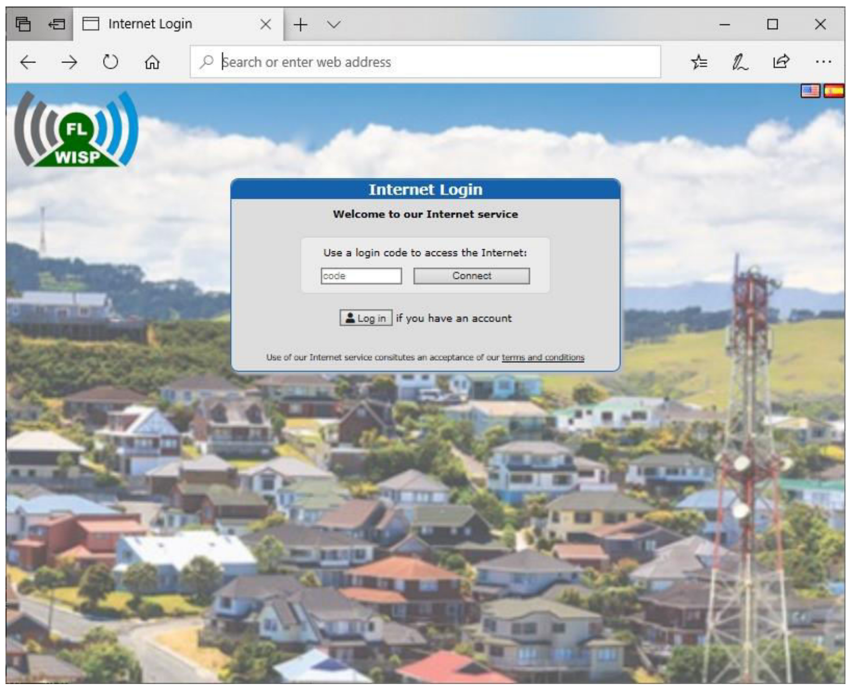


Figure 9.11.3. Example of a captive portal page design.

The third step in the settings process is the configuration of the PayPal® gateway. Customers are able to make credit card payments via the CRM portal, both for the payment of monthly invoices and to purchase access codes for mobile broadband on-demand billing. The WISP must have a PayPal® business account to receive payments using credit cards. A free PayPal® payment account cannot be used to receive credit card payments. The easyWISP system has a PayPal® gateway because PayPal® can be used in over 150 countries around the world. There are many other payment gateways but they are country specific. A future release of easyWISP will include a gateway for Oxxopay so that WISP’s in Mexico and Colombia can receive cash payments through the Oxxopay network.

The PayPal® business account has three parameters which must be entered in the billing settings display; the username, the password and the signature which is an encryption key.

The billing settings data entry box is shown in the following figure.

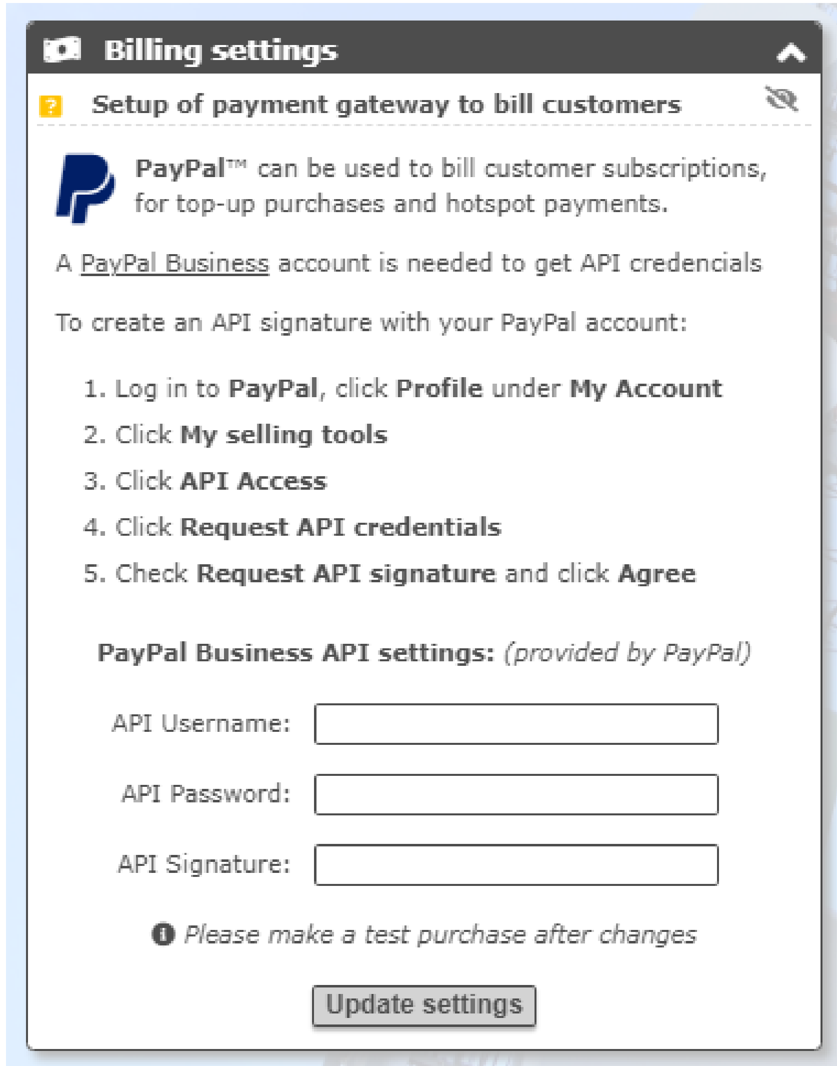


Figure 9.11.4. Settings menu. Configure the PayPal® gateway to receive payments on-line.

The next step in the configuration process is to add the WISP staff to the system. Staff can be added at any time as the WISP business grows. When a member of staff is entered that person has to be given one of the following five roles. There is no limit to the number of people registered for each role.

- Manager
- Technical
- Customer service
- Financial
- Sales

Select staff in the main menu to display the list of staff. Click the button to add a new user.

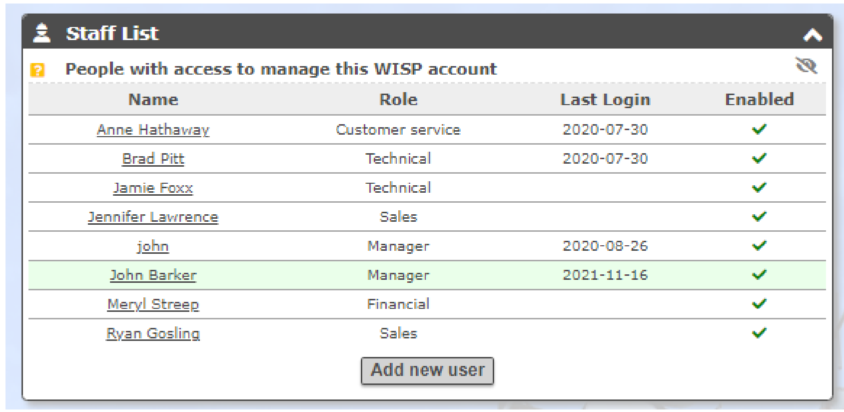


Figure 9.11.5. Staff menu. Display the staff list.

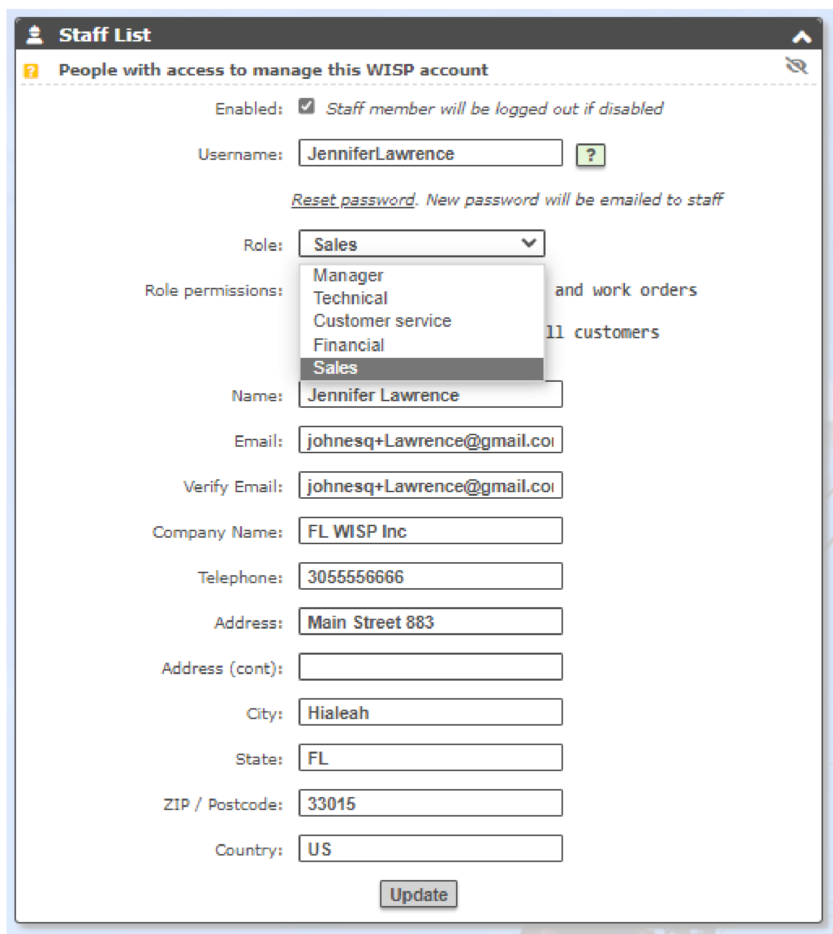
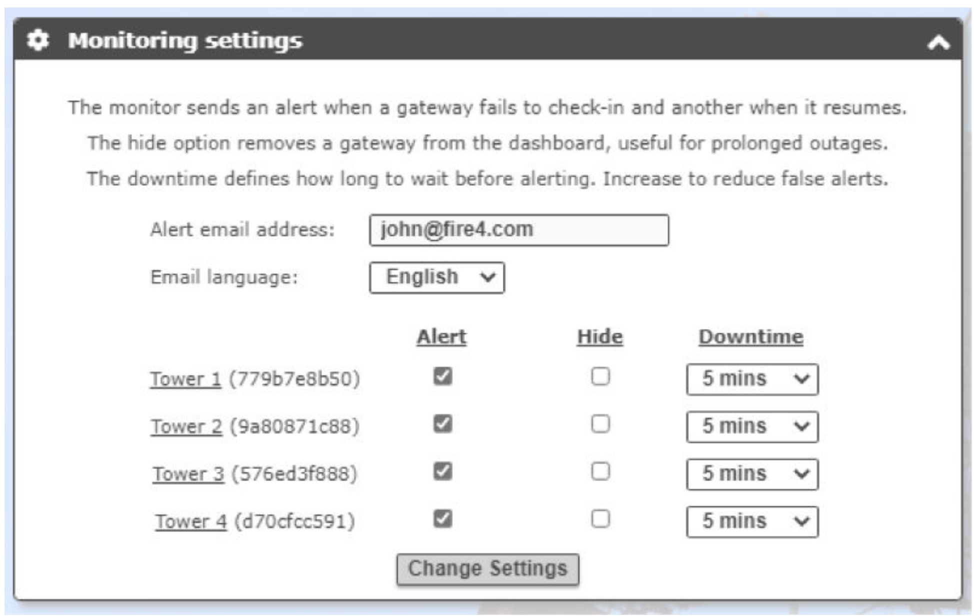


Figure 9.11.6. Staff menu. Add a member of staff selecting the role for that member.

The next step is to configure monitoring for the access control router that was added to the account when it was created. The purpose of monitoring is to send an email alert to the WISP staff if the access control router stops responding to the easyWISP. The reason for a failure to respond might be equipment failure, or a failure in the backhaul link to the tower. The technician will have to do further diagnostics to find the cause of the problem after the alert. When the access control router comes back online a second email message is sent out to advise that the equipment is now connected.

Click on the monitoring menu entry and the access control router gateway will be displayed on the list. Initially there will be only one entry in the list. Enter the email address to which the message will be sent and select the language for the message. Check the alert box for the device and select the downtime from the drop down menu. Downtime is the time that easyWISP waits before sending out an alert message and can be 5 minutes, 10 minutes or 15 minutes. The reason for this is there might be an intermittent connection and so the alarm will not be sent if this occurs. As access control routers are added to the account then monitoring is activated for each.

Figure 9.11.7. Monitoring menu. Activate failure monitoring for the gateway, the access control router.



9.12. Add the rate plans

Select the plans menu entry to configure the rate plans. Rate plans are designed for the WISP's target market and the services must meet the price performance expectations of the prospective customers. The process of calculating the rate plan charges was described in a previous section.

There is no limit to the number of rate plans that can be added and so the WISP can be very flexible with the services offered. Initially it will be useful for the WISP to configure additional rate plans to extend the price performance range of services to test the market and find which plans are the most popular. A price is set for each plan together with the billing cycle duration, usually set for 1 month. The maximum download and upload speeds are added to the plan.

The WISP might wish to set a data cap in addition to the speed limits in the case where the WISP wholesale Internet service includes charges per Gbyte of data. This is the case when using a geo-stationary satellite backhaul. Some wholesale providers also charge per Gbyte of data.

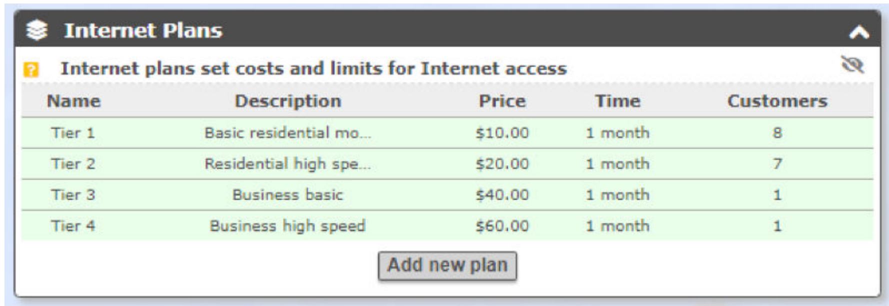


Figure 9.12.1. Click the plans menu entry to see the rate plans that have been configured.

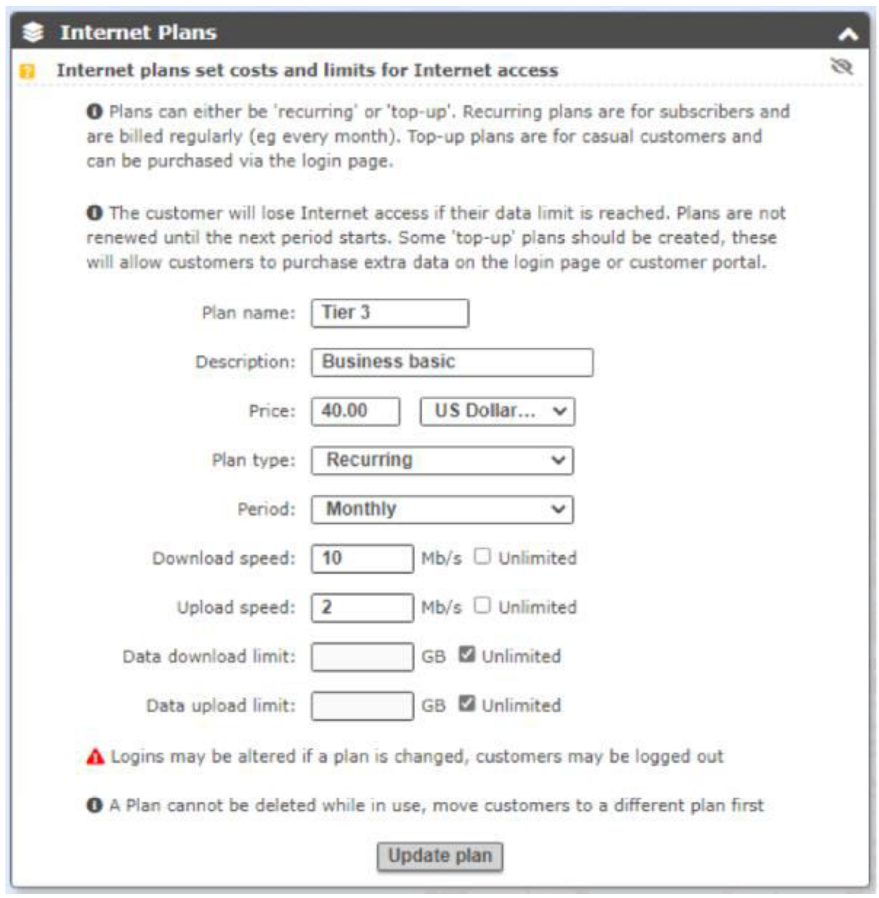


Figure 9.12.2. Click the add new plan button to create a rate plan then complete the information requested. Finally click the update plan button.

The rate plan requires a name and description. Add the charge for the billing period and select the currency of the charge. Select the charge to be recurring or one time, and select the billing cycle period, which is usually monthly. Set the maximum download and upload speeds in Mbits/sec and if a data cap is required set the download and upload data caps in Gbytes.

9.13. Add subscribers

Click the customers menu entry then click add new customer to add the billing information for the first subscriber.

The form shown requires the customer billing information, name, address, telephone and email. Other information that is requested is described on the following pages.

The name of the access control router that will service the subscriber is selected in the gateway drop down menu so that the subscriber access control credentials will be sent to that router.

The MAC address of the CPE is used for subscriber authentication. An additional layer of authentication can be added with WPA2-enterprise authentication with the PtMP wireless communicating with a RADIUS server.

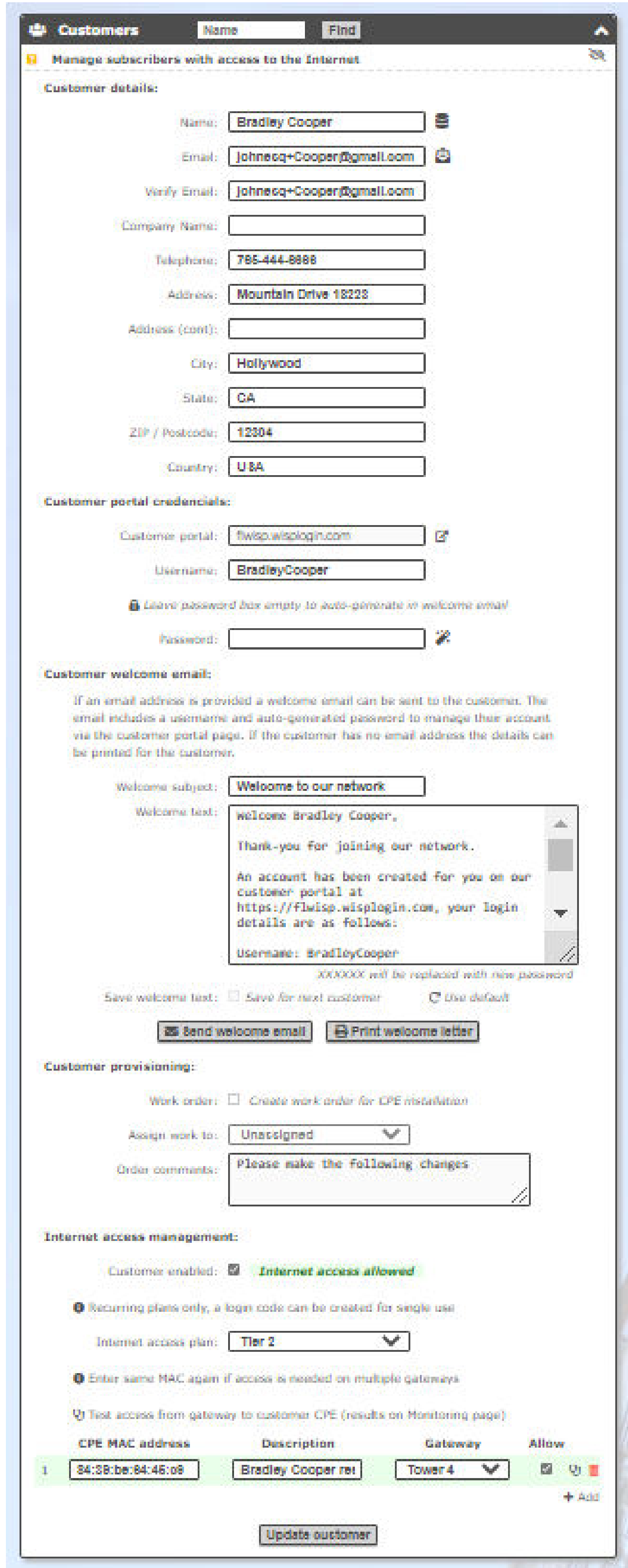


Figure 9.13.1. A completed customer record is shown in the figure.

The sales person will complete the customer account form. It is likely that the sales person is sitting in front of the customer during this process and so can ask the customer for billing information to complete the form.

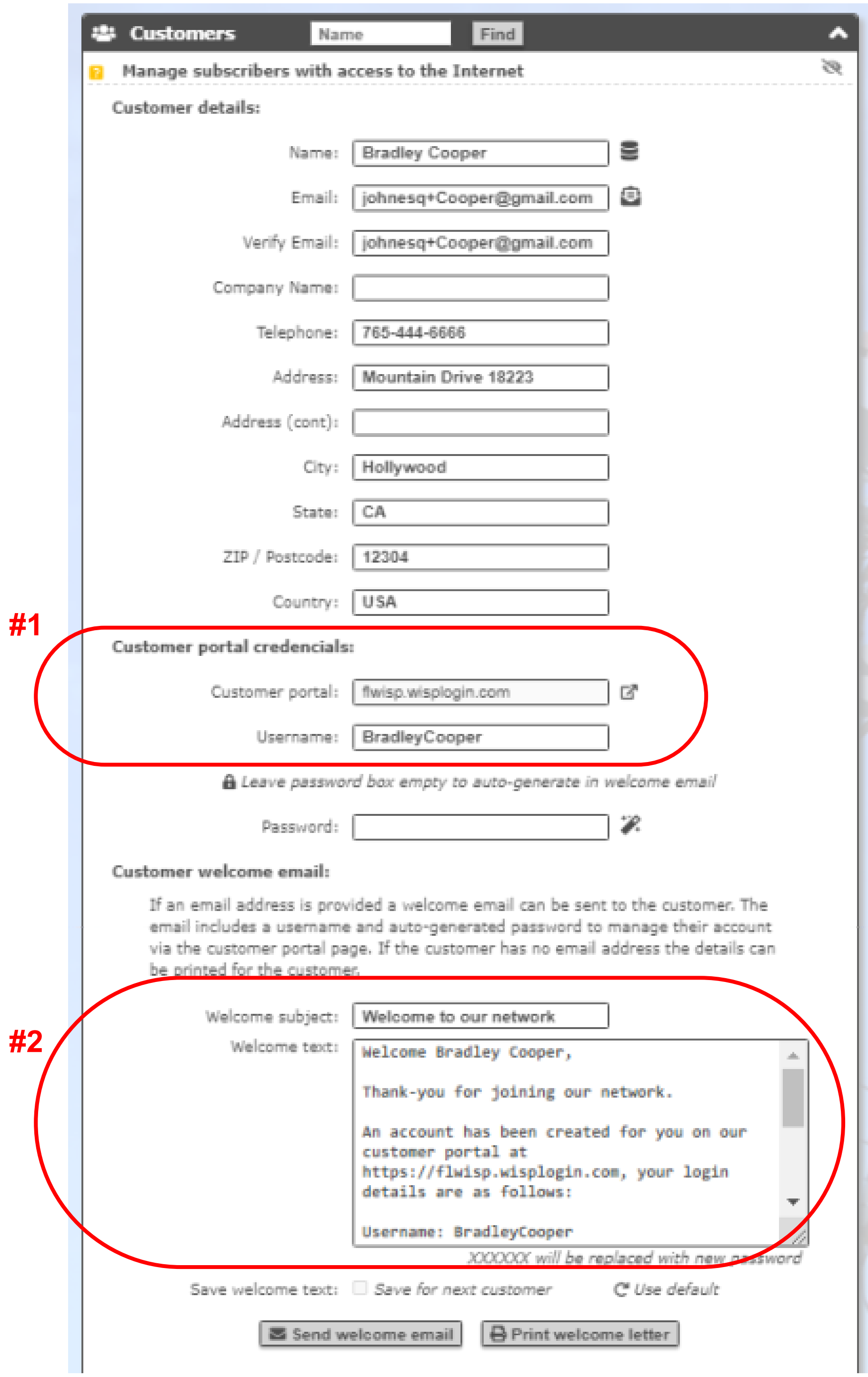


Figure 9.13.2. Important features are highlighted when creating a new customer record.

#1. The customer portal is the subscriber login to the customer relationship management (CRM) system. easyWISP will generate a password and send an email to the customer. The password can be entered manually if desired.

#2. The text of the customer messages can be edited. Click one of the buttons below to either send the message by email or print the message and give to the customer.

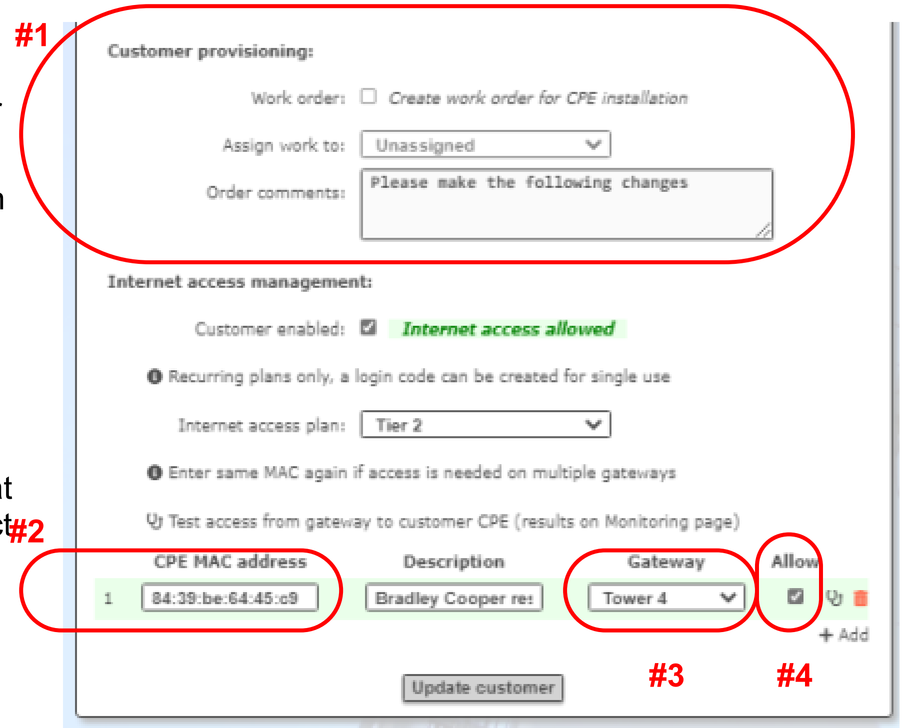


Figure 9.13.3. More important features are highlighted when creating a new customer record.

#1. Initiate an installation work order and direct to a technician.

#2. Configure MAC authentication, set the CPE MAC address.

#3. Set the access control router (tower) that the customer will connect to.

#4. Activate the customer, the billing system will allow the customer to have Internet access.

Click the customer's menu entry to see the list of customers. Billing dates shown in red are accounts past due and the payment has not been received. The accounts with a red '0' MAC address are customers that have purchased the service but have not been installed and so no CPE MAC address has been added yet.

Customers Name Find

Manage subscribers with access to the Internet

Name / Company		Plan	Billed	MACs
Bradley Cooper	✔	Tier 2	2021-10-25	1
Channing Tatum	✔	Tier 1	2021-11-18	1
Christian Bale	✔	Tier 2	2021-11-18	1
Daniel Craig	✔	Tier 2	2021-10-21	1
Dwayne Johnson / DEF News ...	✔	Tier 4	2021-10-25	1
Emma Stone / ES Representa...	✔	Tier 3	2021-10-25	1
Frank / Enterprises LLc	✔	Tier 2	2021-09-27	1
frank jones	✔	Tier 1	2021-10-28	0
George Clooney	✔	Tier 1	2021-10-25	1
Kristen Stewart	✔	Tier 2	2021-11-11	1
Mark Wahlberg	✔	Tier 1	2021-10-21	1
nuvonet / nuvonet	✔	Tier 1	2021-11-01	1
Robert Downey	✔	Tier 1	2021-11-11	1
Sandra Bullock	✔	Tier 2	2021-11-18	1
susan smith	✔	Tier 1	2021-10-28	0
Tom Cruise	✔	Tier 2	2021-11-10	1
Victor / System	✔	Tier 1	2021-08-28	0

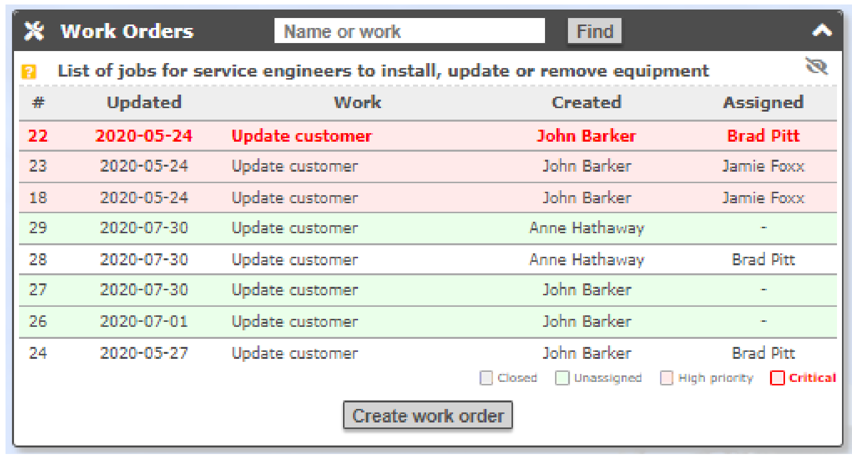
Add new customer

Figure 9.13.4. List of subscribers serviced by all towers. The rate plan that the subscriber purchased is shown next to the subscribers name.

9.14. Work orders for subscriber provisioning

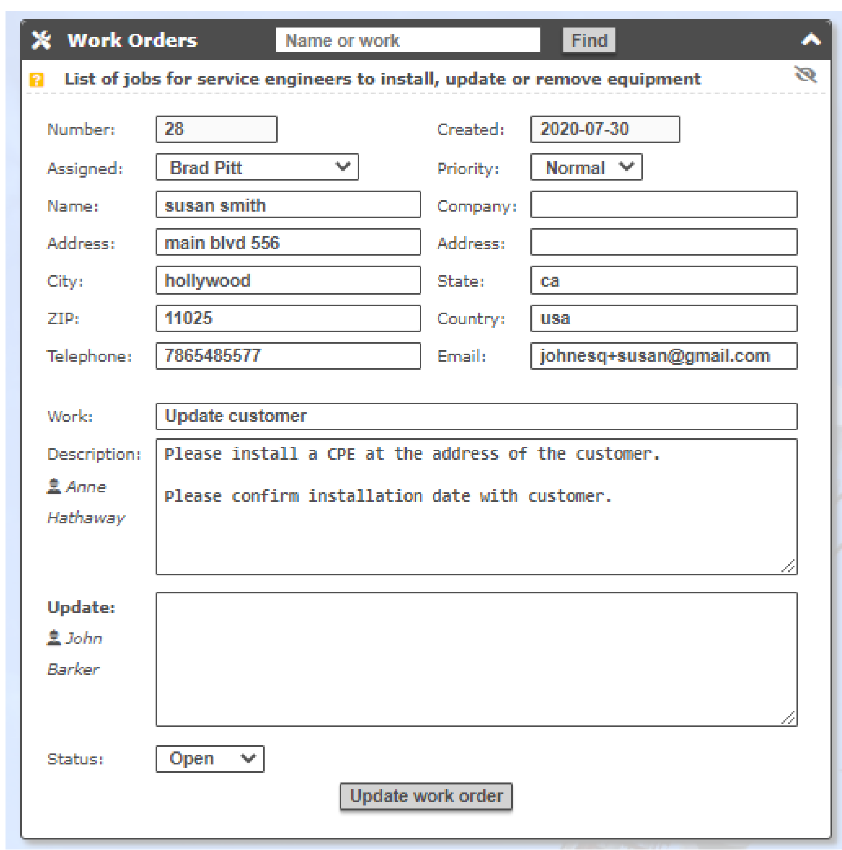
When a customer is added to the service the customer profile box for 'create work order' is checked, which initiates the provisioning process. Select the work orders menu entry to see the list of work orders.

Figure 9.14.1. The list of outstanding work orders showing the status and priority of each.



Click on a work order to see the information in the work order. The first task of technical staff each day is to check outstanding work orders and complete the work required. A new customer installation will require that sales or customer support staff agrees a date and time with the customer for the installation and adds this information to the work order to instruct the technician.

Figure 9.14.2. A work order showing the request for a customer installation.



When the technician goes to the customer premises to install the CPE wireless and wireless router the technician will complete the customer profile by adding the CPE MAC address, the tower name (access control router) if not already entered, and activate the customer. The technician will then demonstrate the Internet connection to the customer and have the customer to sign off on the work order to accept the installation.

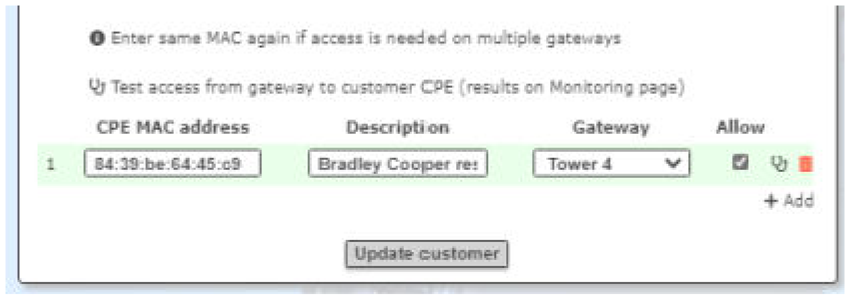


Figure 9.14.3. The customer ‘allow’ box is checked by the technician when the installation is complete.

Most work orders are created when a customer is added to the service, however it is also necessary to create a work order when network maintenance is required or a network component has failed and requires replacing. In this case the manager may create the work order and assign to one of the technicians.

To create a work order select the work orders menu entry then click the button to 'create a work order'. The screen shown below will be displayed and the manager or other employee will complete the information required. The work order is given a title and a description. The priority is assigned to the work order, which can be either; low, normal, high or critical. A failure of a network component will have ‘critical’ selected while a tower inspection might have ‘normal' selected.

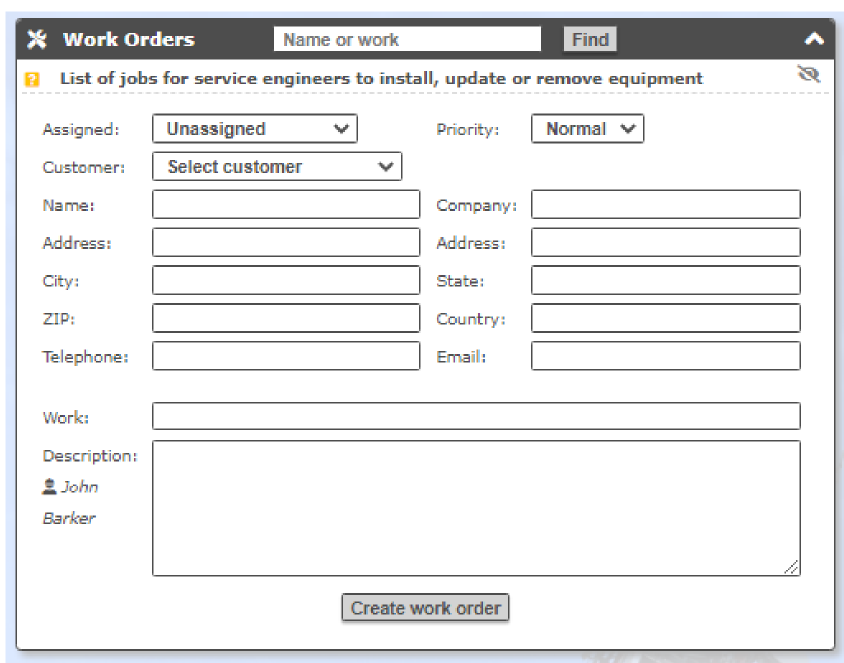
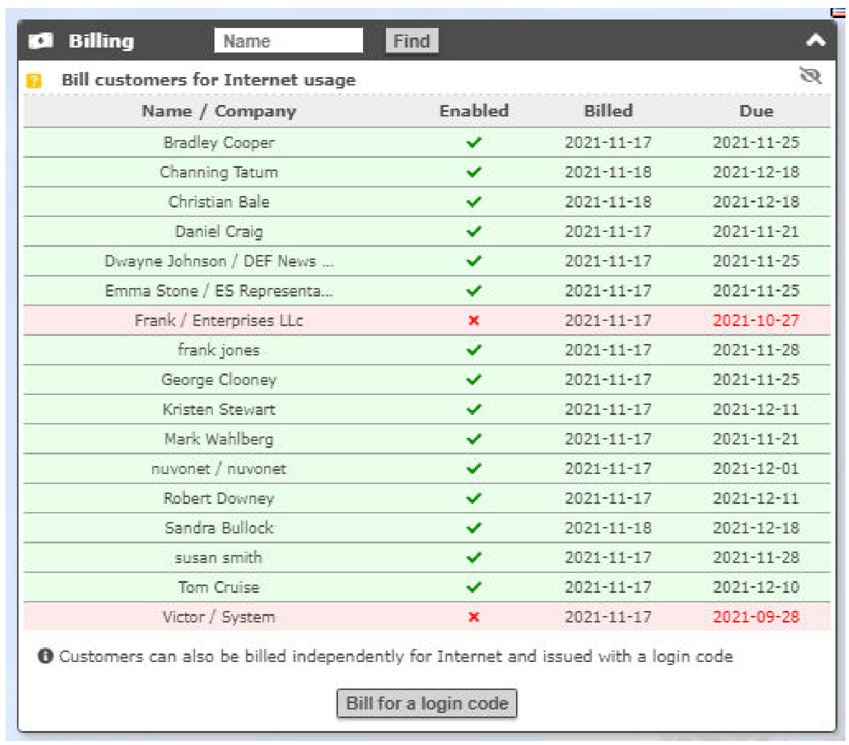


Figure 9.14.4. The form to create a work order.

9.15. Managing the fixed broadband subscriber billing cycle

Fixed broadband customers pay each billing cycle for the Internet service and remain connected to the Internet unless the bill is not paid. A billing cycle is usually set to one calendar month.

Click the menu billing tab to see the first box with the list of subscribers with the billing status of each, and the second box with a list of invoices that have been issued. When the customer is paid up to date the customer entry is shown in green. If the customer bill is past due and payment has not been received then the customer entry is shown in red. One task of the financial staff member is to check this list each day and follow up with customers who have not paid their bill.



Billing | Name | Find

Bill customers for Internet usage

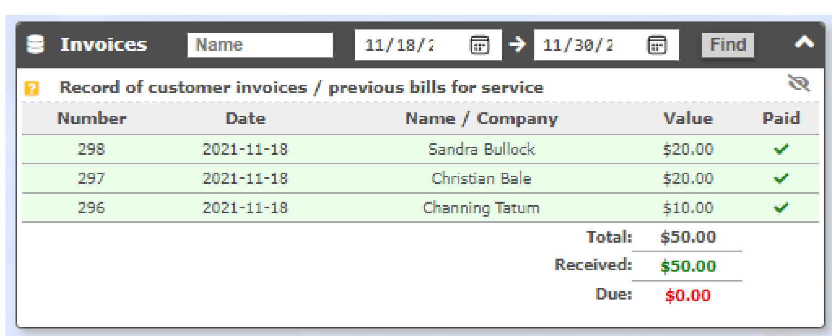
Name / Company	Enabled	Billed	Due
Bradley Cooper	✔	2021-11-17	2021-11-25
Channing Tatum	✔	2021-11-18	2021-12-18
Christian Bale	✔	2021-11-18	2021-12-18
Daniel Craig	✔	2021-11-17	2021-11-21
Dwayne Johnson / DEF News ...	✔	2021-11-17	2021-11-25
Emma Stone / ES Representa...	✔	2021-11-17	2021-11-25
Frank / Enterprises LLc	✘	2021-11-17	2021-10-27
frank jones	✔	2021-11-17	2021-11-28
George Clooney	✔	2021-11-17	2021-11-25
Kristen Stewart	✔	2021-11-17	2021-12-11
Mark Wahlberg	✔	2021-11-17	2021-11-21
nuvonet / nuvonet	✔	2021-11-17	2021-12-01
Robert Downey	✔	2021-11-17	2021-12-11
Sandra Bullock	✔	2021-11-18	2021-12-18
susan smith	✔	2021-11-17	2021-11-28
Tom Cruise	✔	2021-11-17	2021-12-10
Victor / System	✘	2021-11-17	2021-09-28

Customers can also be billed independently for Internet and issued with a login code

Bill for a login code

Figure 9.15.1. The list of subscribers displayed when the billing tab is clicked. Past due late payments are shown in red.

The second box shows the list of invoices issued. The date range can be selected to display invoices for a specific time period.



Invoices | Name | 11/18/2 → 11/30/2 | Find

Record of customer invoices / previous bills for service

Number	Date	Name / Company	Value	Paid
298	2021-11-18	Sandra Bullock	$20.00	✔
297	2021-11-18	Christian Bale	$20.00	✔
296	2021-11-18	Channing Tatum	$10.00	✔
		Total:	$50.00	
		Received:	$50.00	
		Due:	$0.00	

Figure 9.15.2. The list of paid invoices displayed when the billing tab is clicked. Any unpaid invoices are shown in red.

Click on a customer entry to select a billing process for that customer. Select from; create unpaid invoice, create paid invoice, request payment by email message, charge credit card, enable automatic billing.

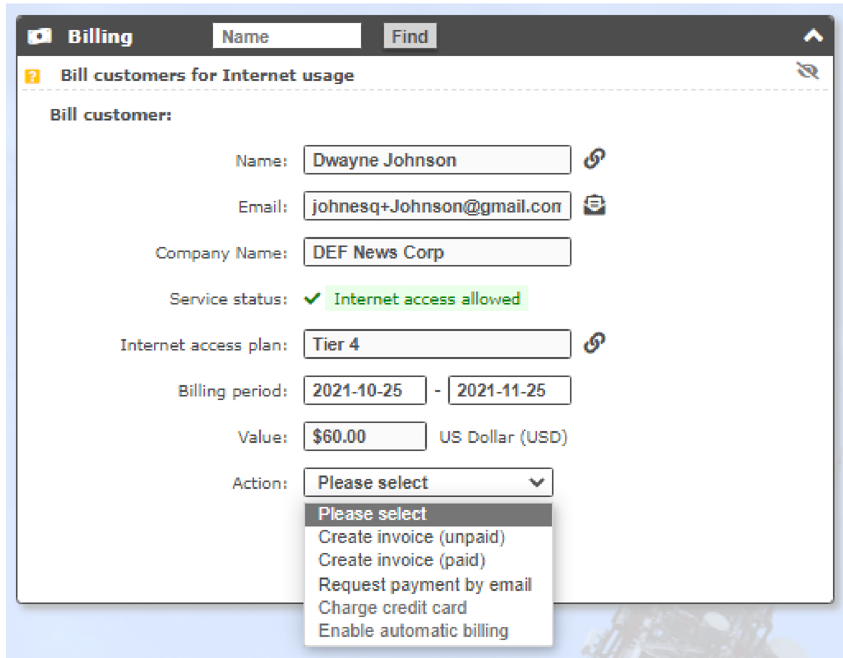


Figure 9.15.3. The customer billing entry is selected for processing. Choose one the options in the drop-down menu. For example print an unpaid invoice to send to the customer, and when the customer's payment is received generate a paid invoice, which also sets the account as paid.

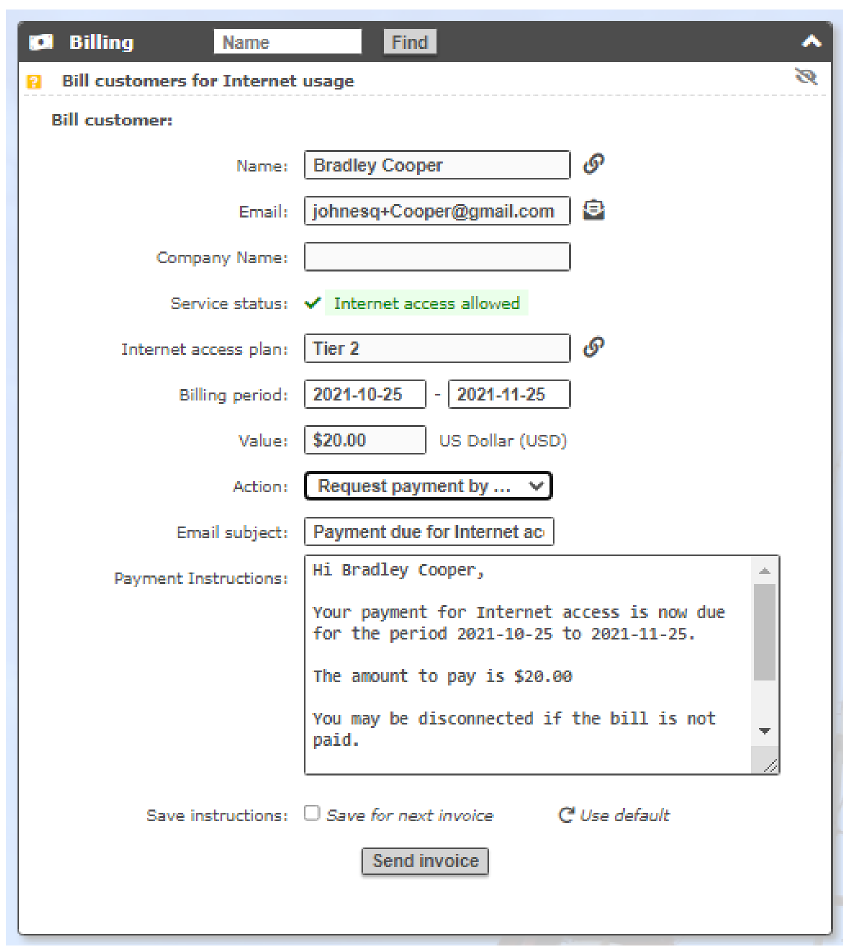
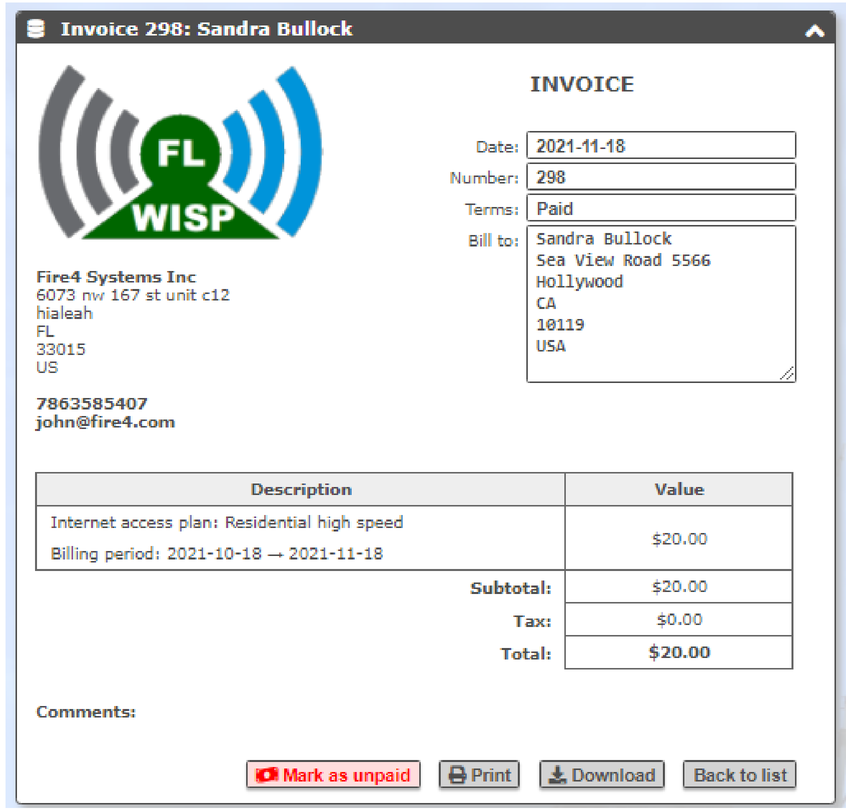


Figure 9.15.4. Select the option to send a request for payment by email, the message can be edited and saved then used as the default message to customers.

Figure 9.15.5. Select the option to print an invoice. The invoice can be printed for posting or downloaded to send as an email attachment.



Each day the financial staff must check the list of subscribers for billing due dates. The staff will send out an invoice before the due date, this period depends on the WISP, and can be 15 days. The financial staff will check each day for payments received and note a payment receipt on the customers account by clicking on the paid invoice. The customer can access the paid invoice that is generated via the CRM portal login. If a customer fails to pay an invoice by the due date then the customer looses access to the Internet because the billing system disables access, but the customer does have access to the CRM portal. When the customer account is marked as paid the Internet access is restored by the billing system.

The billing system is very easy to use and requires very little staff training. The manager must check the billing display daily to follow up with staff procedures.

9.16. Managing the mobile broadband on-demand billing

The mobile broadband on-demand billing requires access codes to be generated by the WISP then downloaded and saved in a comma separated value (CSV) format. The access codes can then be printed onto vouchers or scratch cards for sale to customers. Customers can also purchase access codes through the CRM portal and pay on-line using a credit card.

The mobile broadband service will be provided via an unencrypted wireless access point and will be a connection over a short range of a few hundred meters, as customers will be connecting with mobile devices.

Select the codes option in the menu then select the access control router gateway where the code will be used.

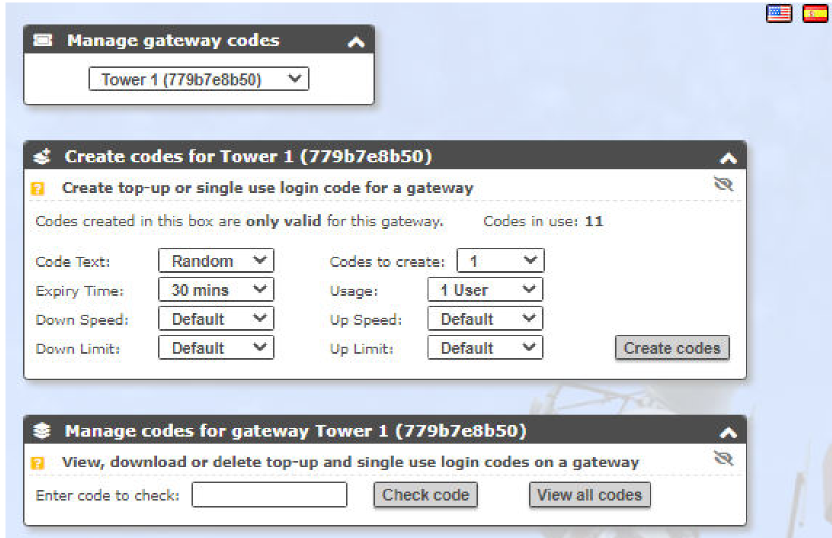


Figure 9.16.1. Select the codes menu option then select the access control gateway.

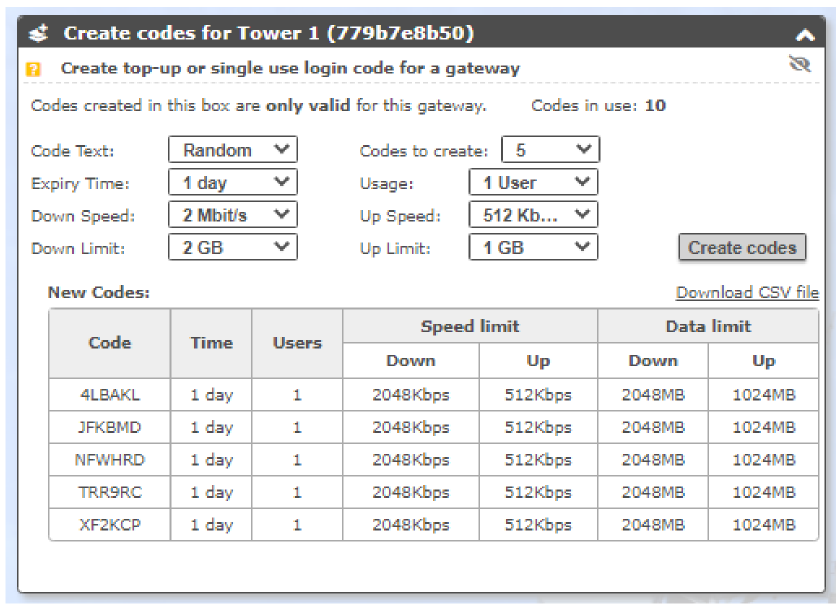


Figure 9.16.2. Select the parameters for the codes to be generated; the type of code (random or custom), the number of codes if random, the code name if custom, the code duration, the number of users per code, the maximum download and upload speeds, and the download and upload data limits. Then click the 'create codes' button.

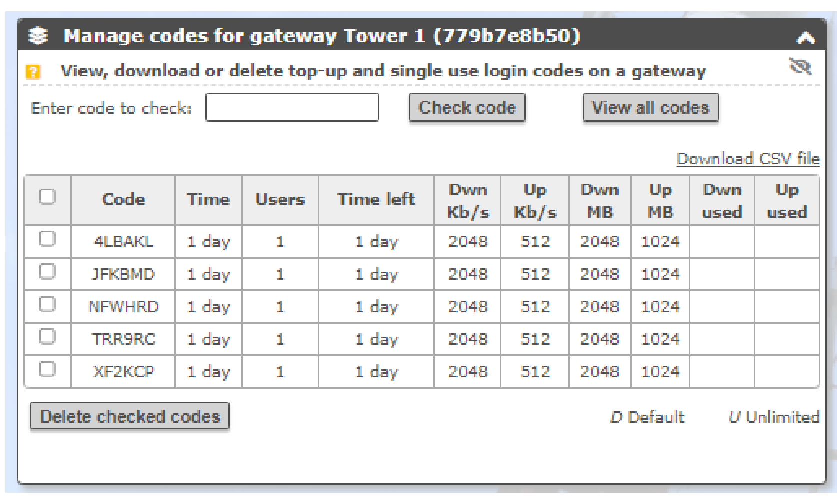


Figure 9.16.3. Click the 'view all codes' button to show a list of all codes that have been generated. Download the codes for printing.

9.17. Gateway configuration and traffic information

Each access control router gateway can be monitored and configured. Click the 'gateway' menu entry then select the gateway to be displayed from the drop down list. This screen is also used to find a gateway, add a gateway and delete a gateway. When a gateway has been selected the configuration parameters for that gateway are displayed.

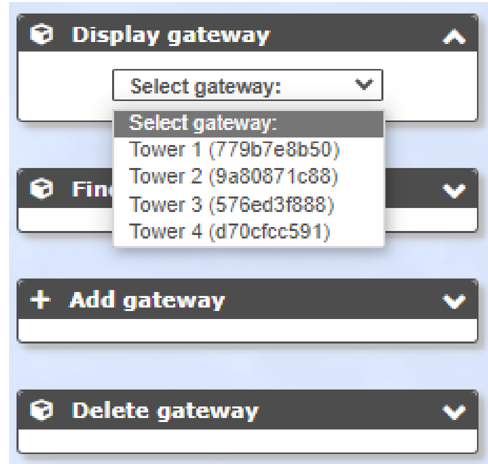


Figure 9.17.1. Gateway selection.

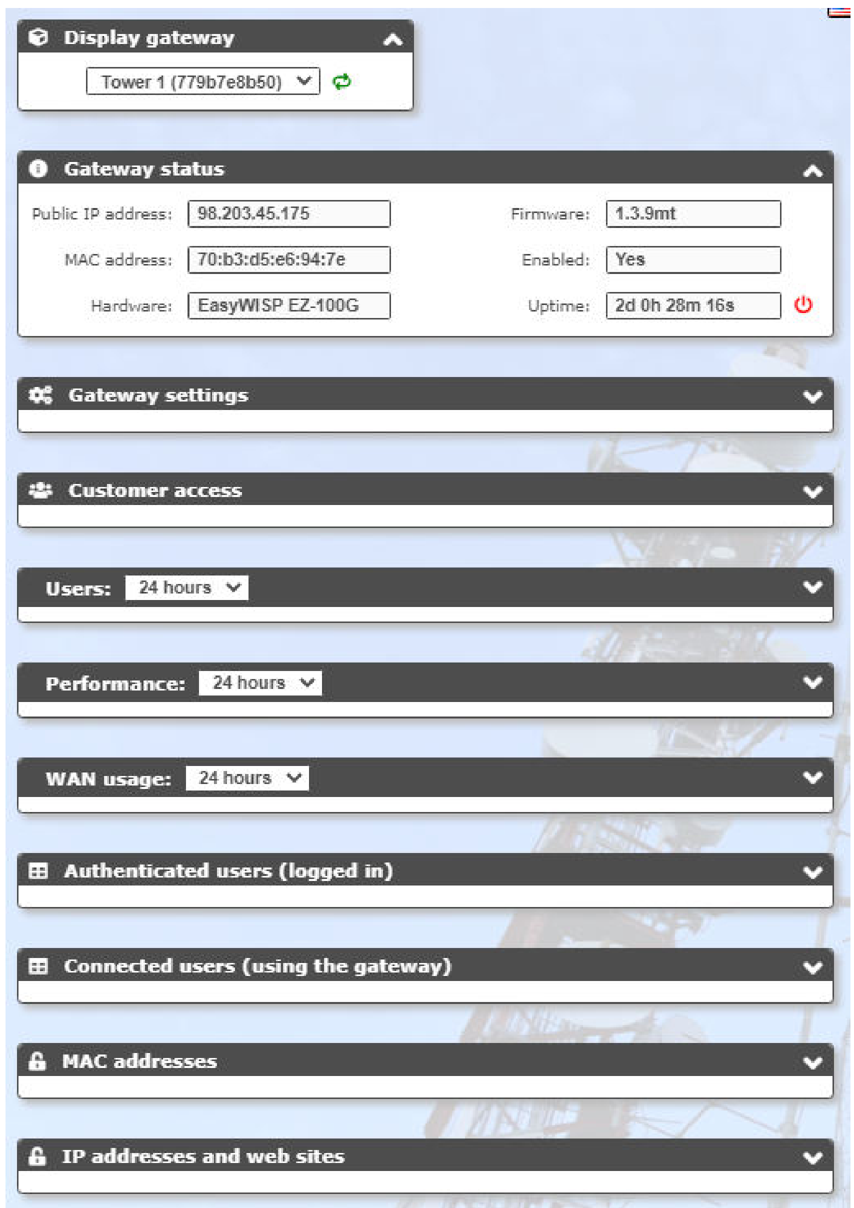


Figure 9.17.2. The access control router gateway parameters are displayed as a series of boxes that can be opened as required. The access control router gateway status box is shown opened to display the basic parameters of the gateway. Note that the access control router gateway firmware is updated automatically by the cloud4WUSP system. Each box is described in the following pages.

The gateway settings box permits the network configuration parameters of the access control router to be changed. Each gateway is given an easily recognizable name (e.g. Tower 1) and the password of the gateway can be changed.

The WAN port settings will have been configured when the easyWISP or Mikrotik access control router was installed and can be modified here if required. The WAN settings will have been set either for a static public IP or as a DHCP client installed behind a network router with a private address range. If a mistake is made when modifying the WAN settings then contact with the device will be lost and the technician will have to go to the tower to reset the WAN settings.

The LAN port settings always provide a DHCP service for CPE devices configured as routers. The CPE devices can be configured with static IP's however each IP must be within the LAN subnet range but outside the DHCP range. The DHCP range will require changing if CPE devices are configured with static IP's.

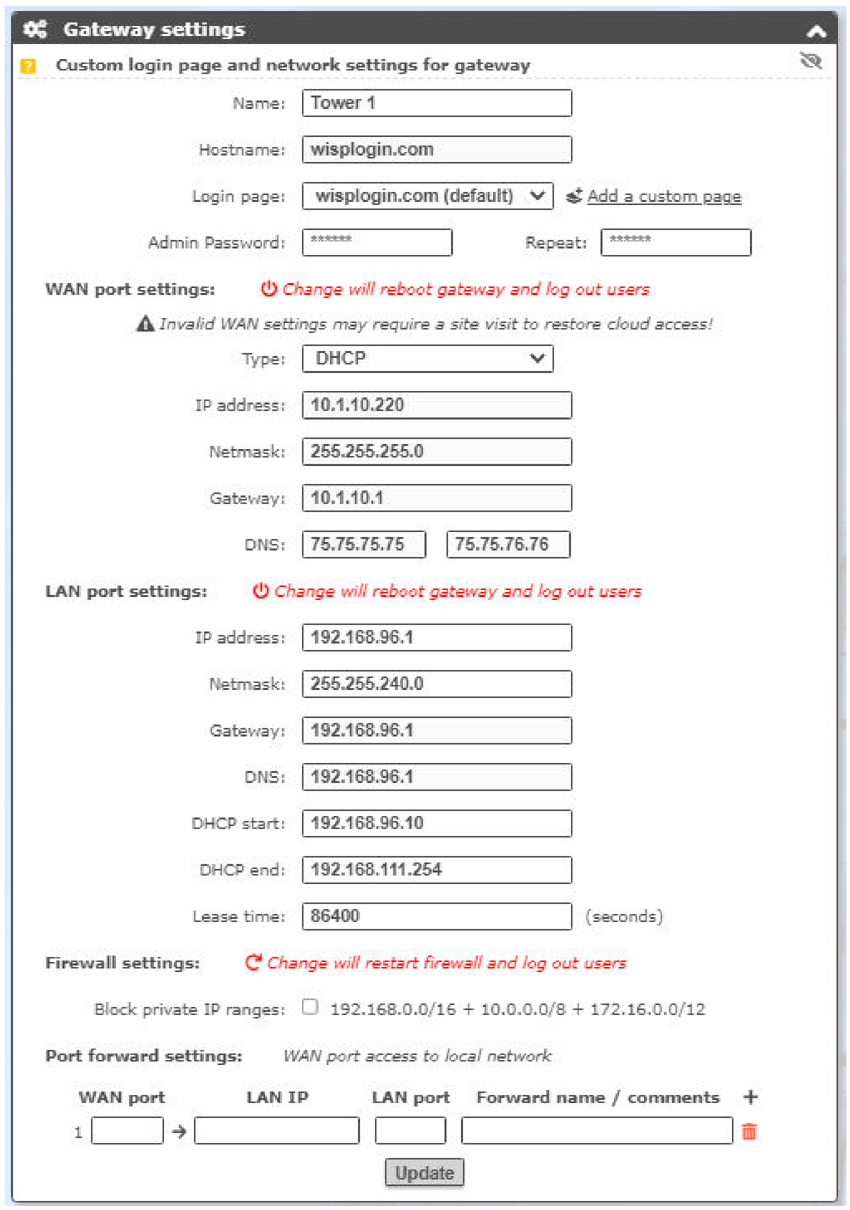
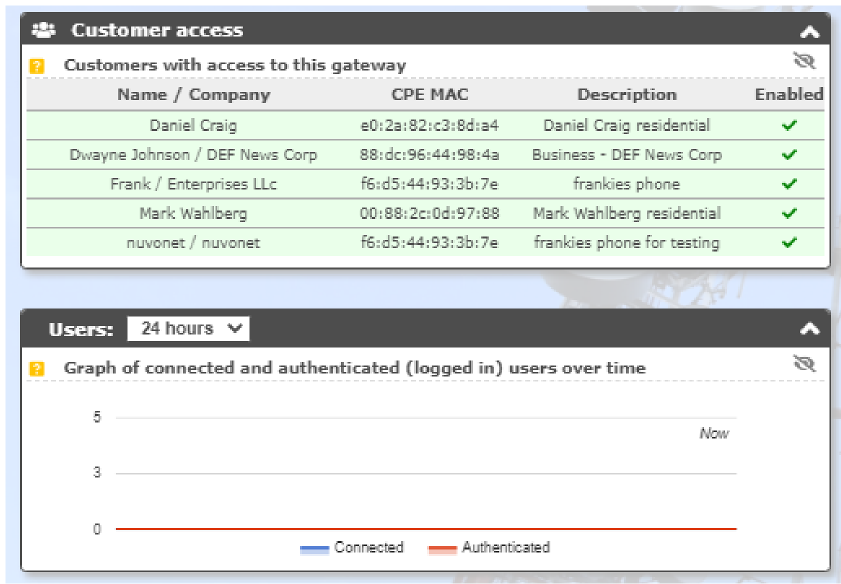


Figure 9.17.3. The access control router gateway settings box permits changes to the gateway parameters.

The gateway settings box has two additional configurations. The first configuration will block access to private IP ranges in the WAN circuit and is useful if the WAN port is connected to a router and is sharing a private IP range with other devices. The second configuration is to add a port-forward rule to permit wireless access points and CPE devices to be accessed remotely where the WISP requires access to the device UI for configuration purposes. Up to 100 port-forward rules can be added.

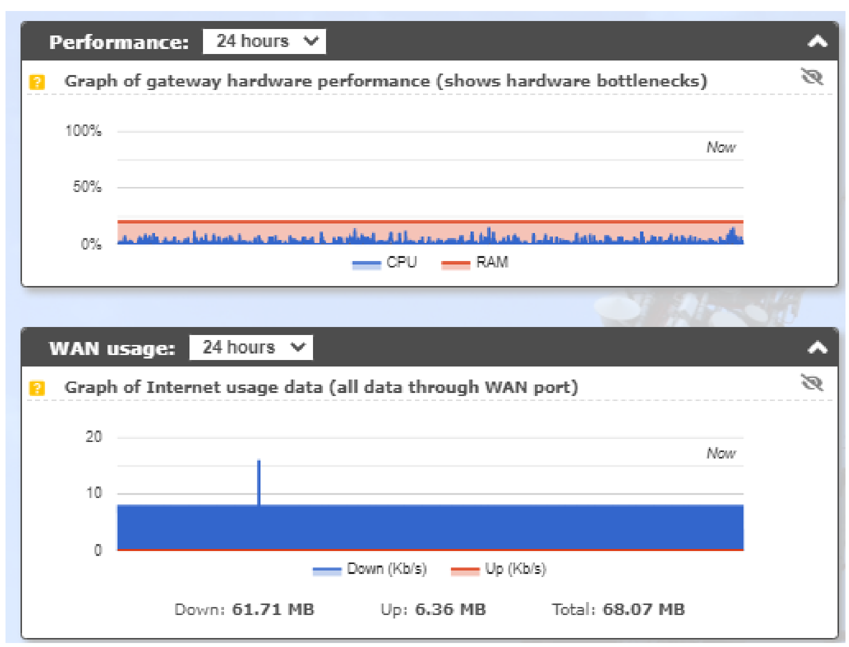
The information boxes shown below illustrate the subscribers and authentications with time.

Figure 9.17.4. The list of subscribers associated with the tower access control router gateway and a graph showing the number of authenticated subscribers with time. The time axis can be selected between 1 hour to 1 week.



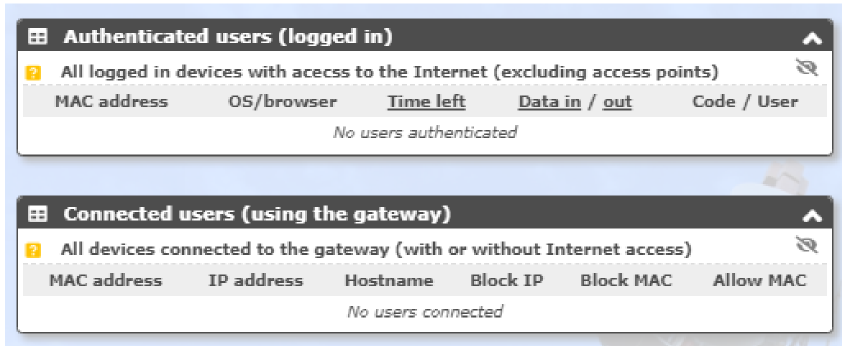
The graphs shown below illustrate the performance of the gateway and backhaul connection, and can be used to identify bottlenecks in the network and indicate where circuit upgrades are required.

Figure 9.17.5. Graphs showing performance of the gateway processor in % of maximum capacity with time, and a graph of WAN port bandwidth use with time. The time axis can be changed from 1 hour to 1 week.



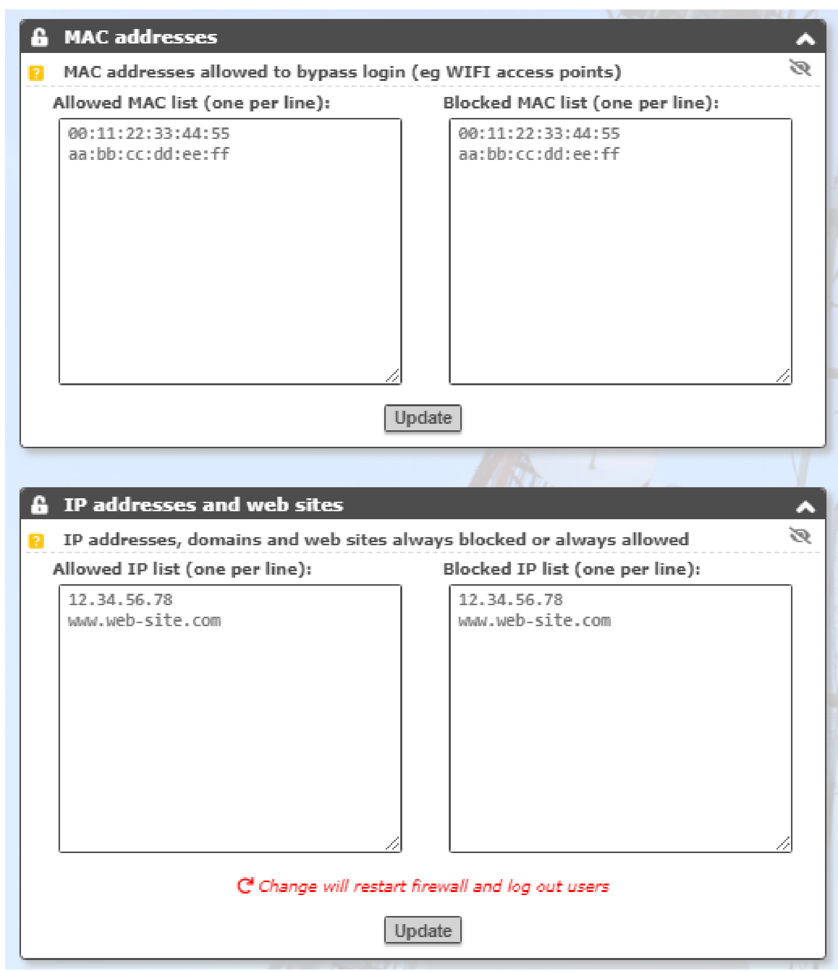
The boxes show below list the subscribers that are connected to the network and the subscribers that have been authenticated. Connected means that the CPE is visible to the access control router, while authenticated customers are communicating over the network and their identity has been authenticated.

Figure 9.17.6. Lists showing authenticated and connected subscribers.



The tables shown in the figure below are the MAC blocked and allowed tables that are configured for the access control router, and the IP or domain allowed and blocked addresses for the access control router.

Figure 9.17.7. The upper box is the list of allowed and blocked MAC addresses, and the lower box shows the allowed and blocked IP or domain name addresses.



9.18. Monitoring of network failures

The configuration of the access control router gateway monitoring was described during initial setup. The messages that are sent to the WISP administrator in the case of failure are shown below.

Figure 9.18.1. Activate alerting in the case of access control router gateway failure, which may be due to a failed device or a tower WAN circuit failure.

Figure 9.18.2. Message sent to the WISP administrator when the easyWISP system looses contact with an access control router gateway.

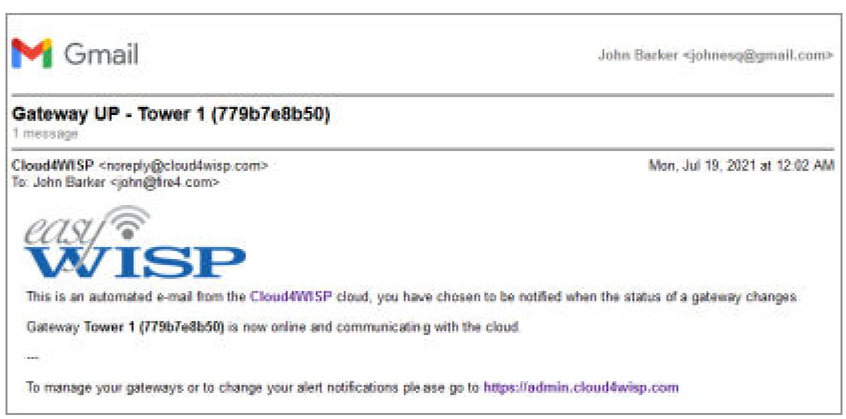


Figure 9.18.3. Message sent to the WISP administrator when the easyWISP system restores contact with an access control router gateway.

9.19. The subscribers view of the Internet service (the CRM portal)

The customer relationship management (CRM) portal serves a number of purposes. First the customer is redirected to an information screen if the customer's account is not paid, or else there is a technical problem and the access control router has no connection to the Internet. The WISP might have set a data cap with the subscribers account so if the data cap is exceeded the information screen is displayed.

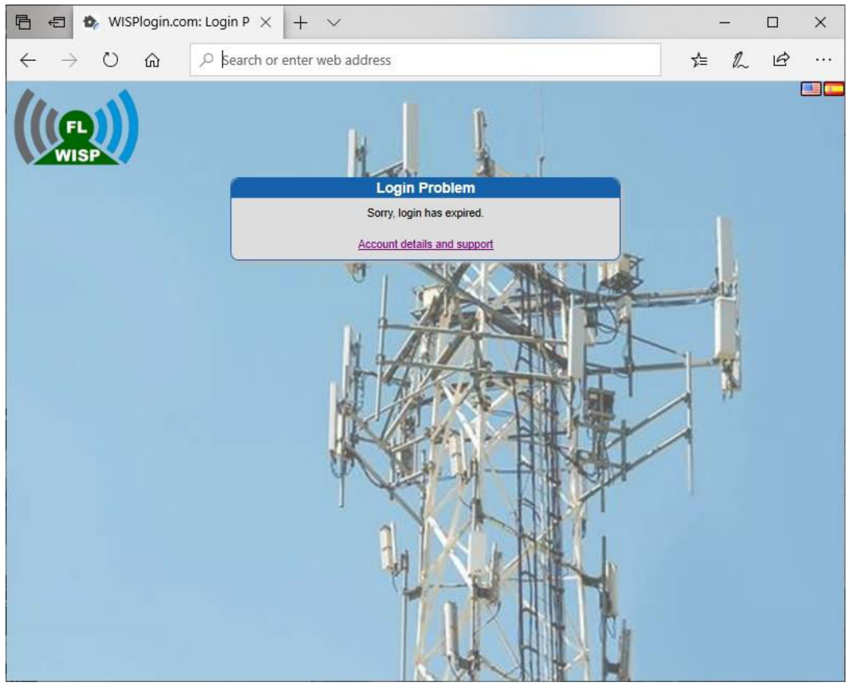


Figure 9.19.1. The screen that the subscriber will see when the account is past due. The billing system has disabled the subscriber and the subscriber is re-directed to this page.

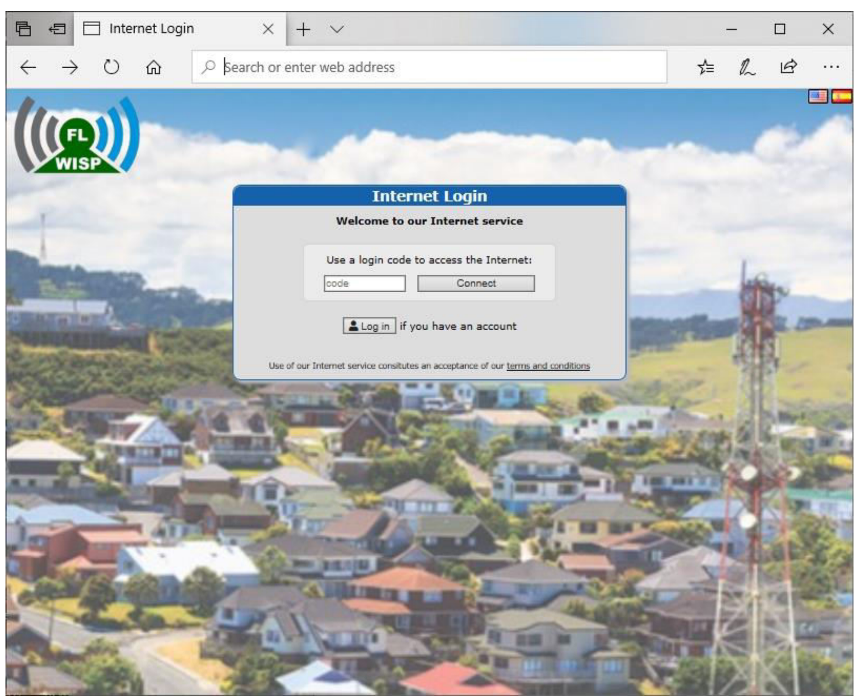


Figure 9.19.2. If a data cap is configured for the subscriber and the data cap is exceeded then this is the screen that the subscriber will see.

When the subscriber account is created the subscriber receives a message with the CRM portal login user name and password, this is either sent to the customer via email or printed out and given to the customer. An example of the email message is shown in the next figure.

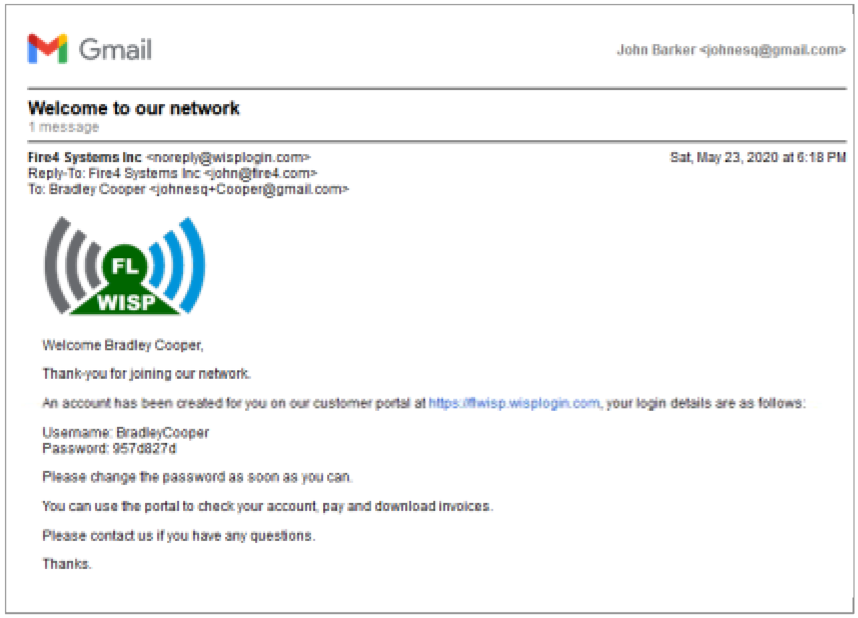


Figure 9.19.3. An example of the message that the subscriber receives when the account is created, advising the username and password to access the CRM portal together with the portal URL.

Typing the URL into the browser tab opens the subscriber CRM captive portal login page.

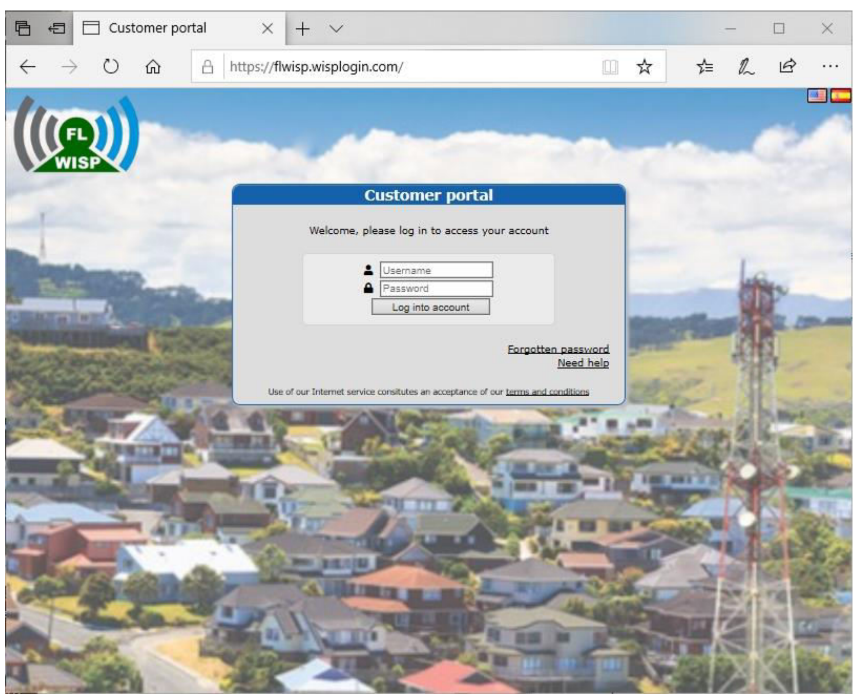
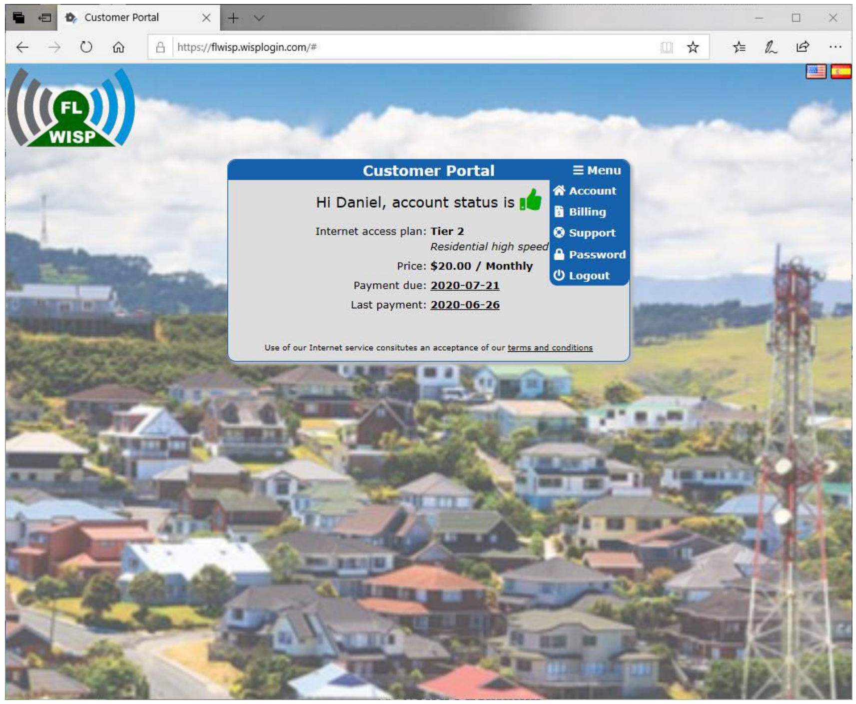


Figure 9.19.4. The CRM portal login screen using the login credentials provided in the message.

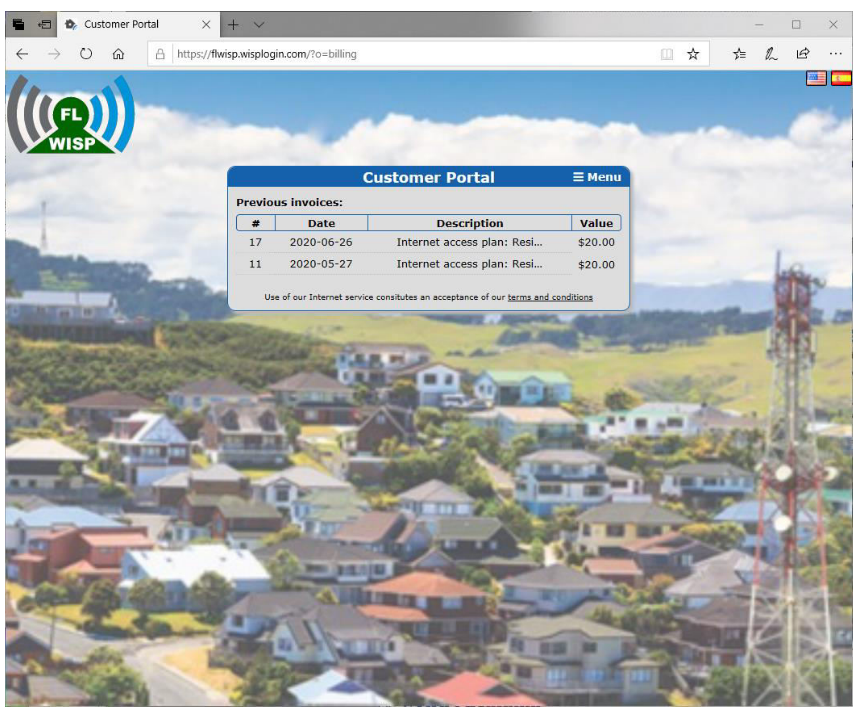
When the subscriber logs in to the CRM portal there is a menu with several options; view account information, see billing information, which includes downloading invoices, open a customer support request, change the password and logout.

Figure 9.19.5. The CRM screen after login showing the subscriber's account status.



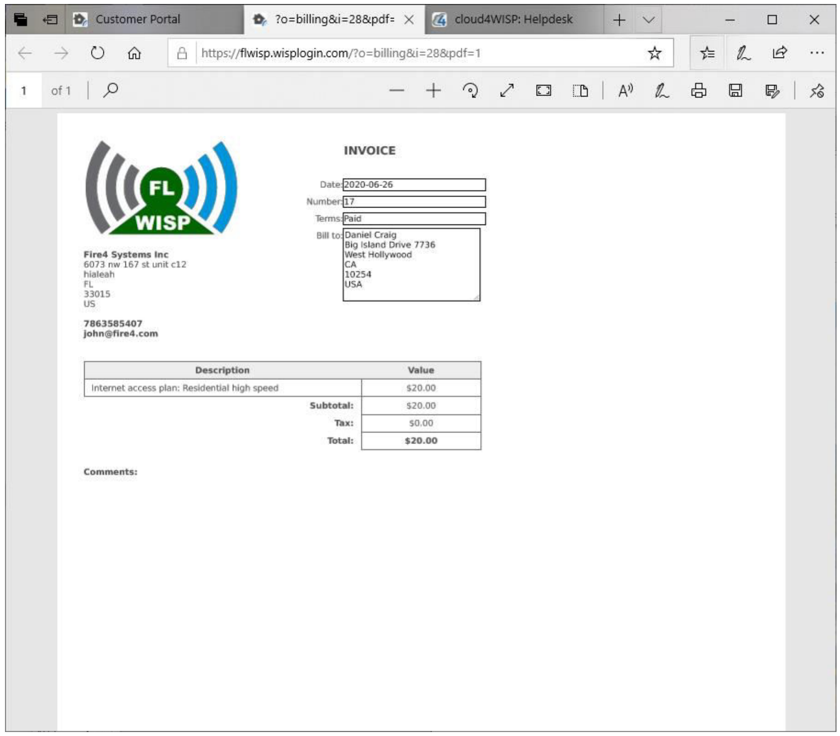
Selecting the billing menu option lists the invoices issued for the account.

Figure 9.19.6. Click on any invoice to open and view the invoice.



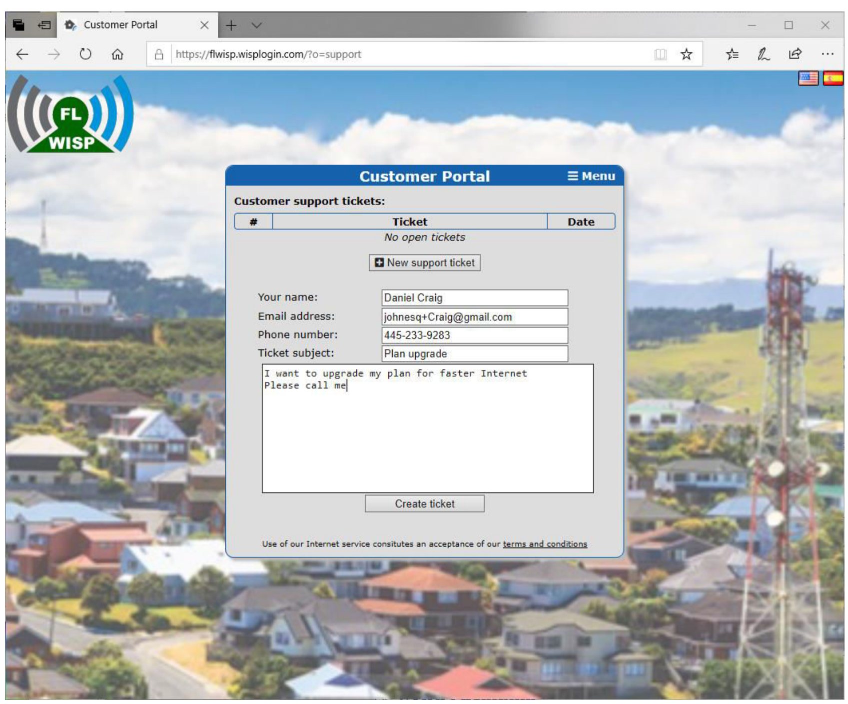
Click on any invoice listed in the billing menu to open it in a new browser window. The invoice can be printed or saved on the subscriber's computer.

Figure 9.19.7. Display an invoice selected from the list of invoices.



The subscriber can click on the support menu entry to open a customer support request, which is sent to the helpdesk.

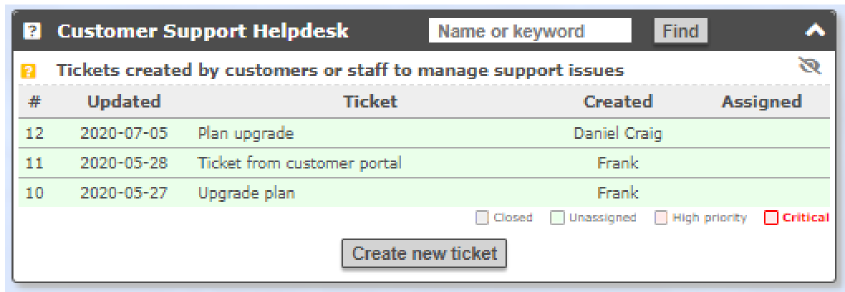
Figure 9.19.8. Entry of information for a customer support request.



9.20. Helpdesk

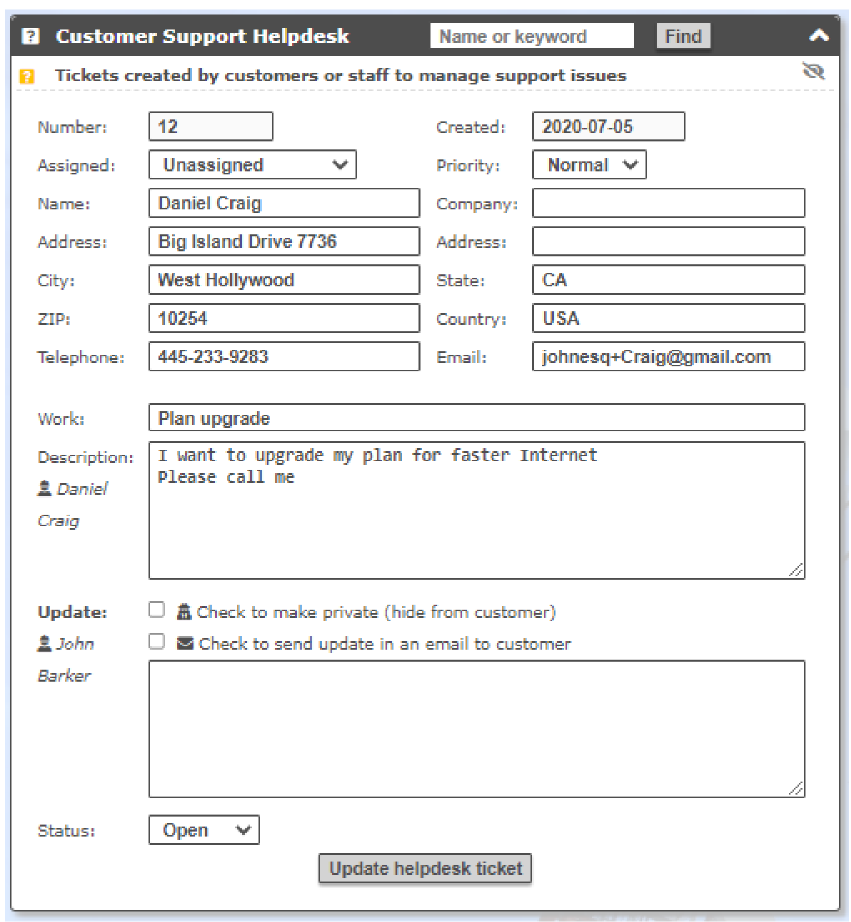
Click on the helpdesk menu entry to view the customer support staff screen. The helpdesk shows a box with open support tickets that are sent by subscribers using the CRM portal. Click on any ticket entry to open a box that will display the ticket.

Figure 9.20.1. The list of open tickets is shown, each can have a priority set according to the urgency of the issue.



When the ticket is opened by the customer support staff then customer support may be able to answer the question, or the question may need assigning to another member of staff; the financial staff for billing questions, the sales staff for upgrades and new services, and the technical staff to answer technical issues. The reply to the customer can be sent via an email or via a call. Check the box to send an email.

Figure 9.20.2. The support ticket with the request from the subscriber.



The customer support staff also receives telephone calls from customers. A common type of call is a complaint that the customer has no Internet access. The customer support person can check the circuit through to the customer CPE wireless using a feature on the gateway configuration screen. If the response shows that the circuit to the customers CPE is good then the problem is the network at the customer's premises. If a problem is detected communicating with the CPE then the customer support staff must open a work order for the technical staff to locate and correct the network problem. If the problem is found to be at the customer's premises then it is usual to request the customer to pay a service charge in order to have a technician go to the customer's premises to correct the problem. If the customer agrees to the charge then a work order can be opened for technical staff to proceed to the customer's premises to repair the fault.

Figure 9.20.3. Gateway configuration screen showing circuit test to CPE.

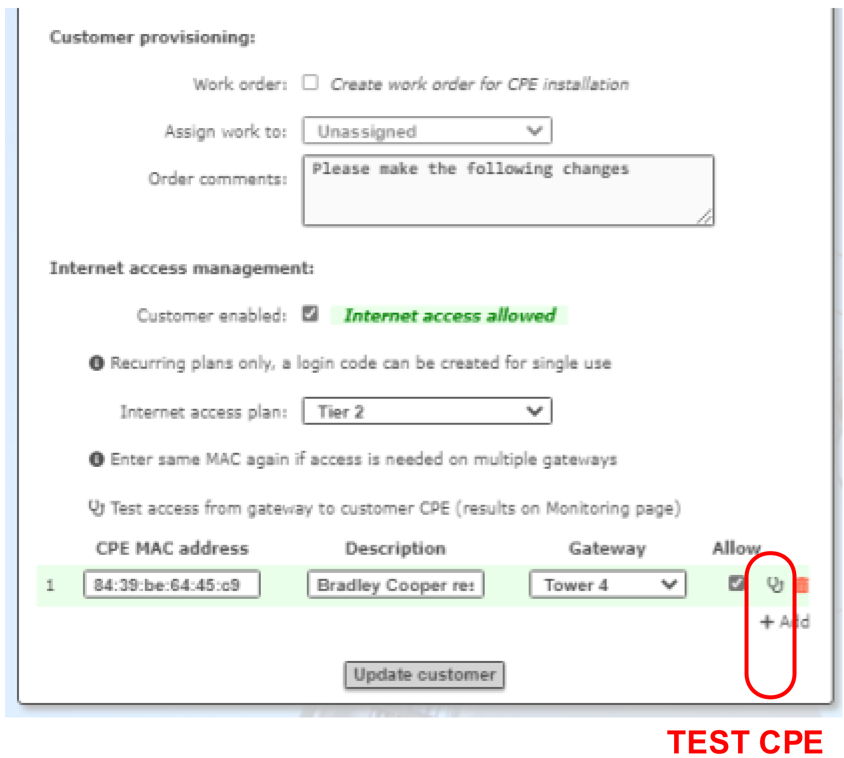
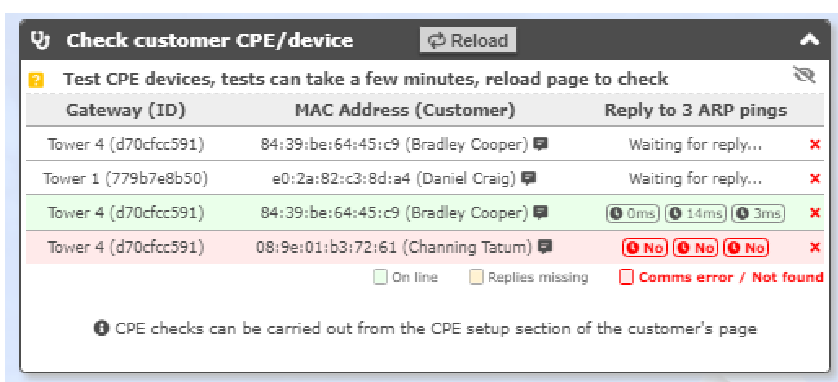


Figure 9.20.4. Check customer CPE display showing the result of the customers CPE circuit test.



9.21. Add gateways: access control routers

Each time that a PtMP tower is added to the network an access control router gateway will be installed on the tower. The access control router gateway is added to easyWISP configuration as a PtMP tower and then new subscribers can be added to this tower. Click the gateways menu tab to display, find, add, or delete access control router gateways.

The display gateway box has a drop down menu to select any of the access control router gateways associated with the account for display. The find gateway box can locate a gateway using the ID or using the name given to the gateway. The add gateway box is used to enter the ID of a gateway that is being added to the account. The gateway is then selected for configuration. The delete gateway box permits a selected gateway to be removed from the account.

Figure 9.21.1. Click the gateway menu entry to add a new access control router gateway ID then select the gateway for configuration.

After the access control router gateway ID is added the device configuration information is loaded to the cloud and is shown in the configuration box. In most cases the only additional configuration required is to give the device a name that is relevant to the network installation, for example ‘Tower 4' in the example shown below.

It should not be necessary to change the LAN or WAN settings and care should be taken if these settings are changed as customers will loose the Internet connection temporally, and an error with the WAN setting will stop Internet access for customers connected to this router. The technician will have to go to the tower site to manually reconfigure the unit.

The WISP may want to add port forward rules for remote access to the PtMP wireless access point UI’s and the CPE device UI’s. Device UI IP's should be configured sequentially within the subnet range but outside the DHCP range. It will be necessary to change the DHCP range to add more than nine port forward rules.

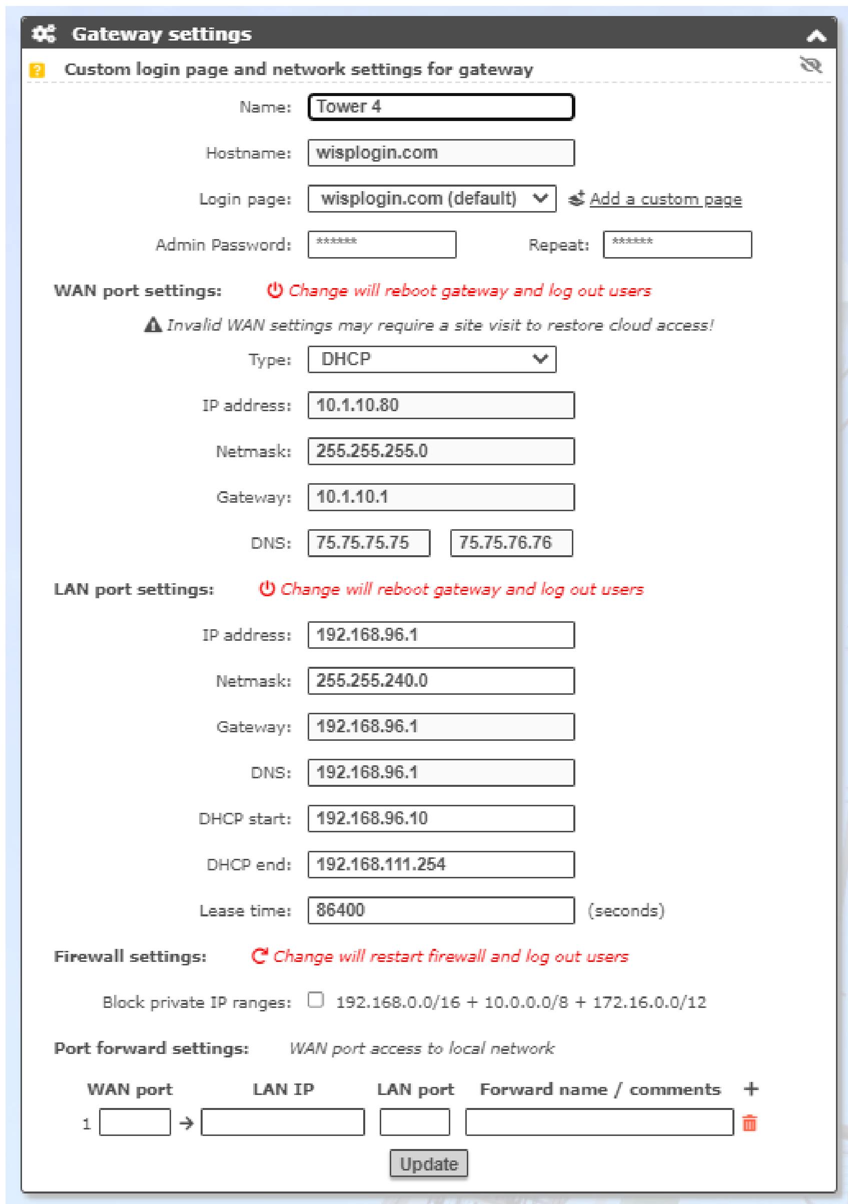


Figure 9.21.2. The access control router gateway settings can be changed using the gateway settings box.

9.22. WISP business operations

The WISP has four daily department activities; sales, financial, technical and support. Each activity may have multiple members of staff involved in the activity. The manager also has several activities to supervise staff. A daily flow diagram is shown for each department activity and also for the manager.

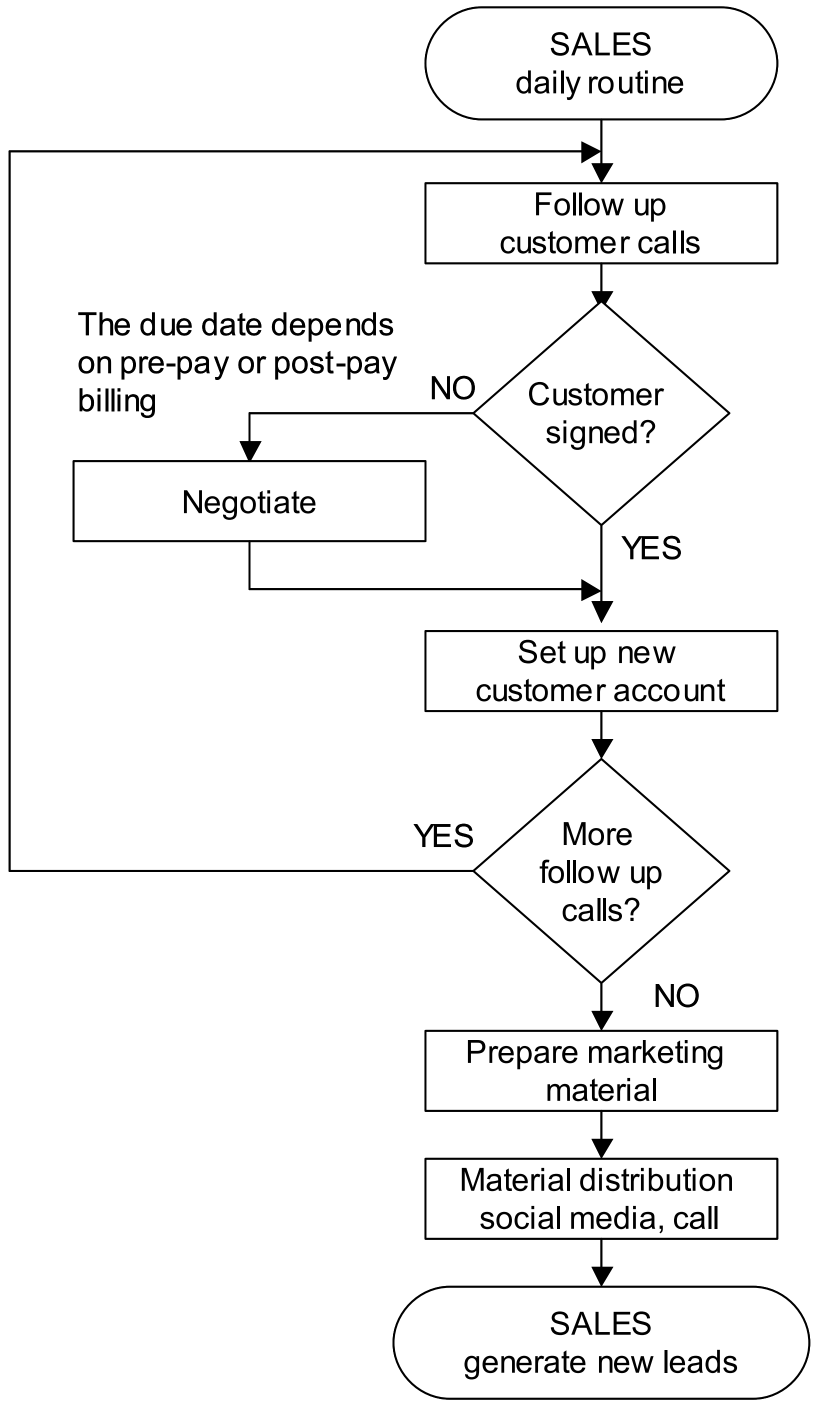


Figure 9.22.1. Flow diagram for the sales staff daily tasks.

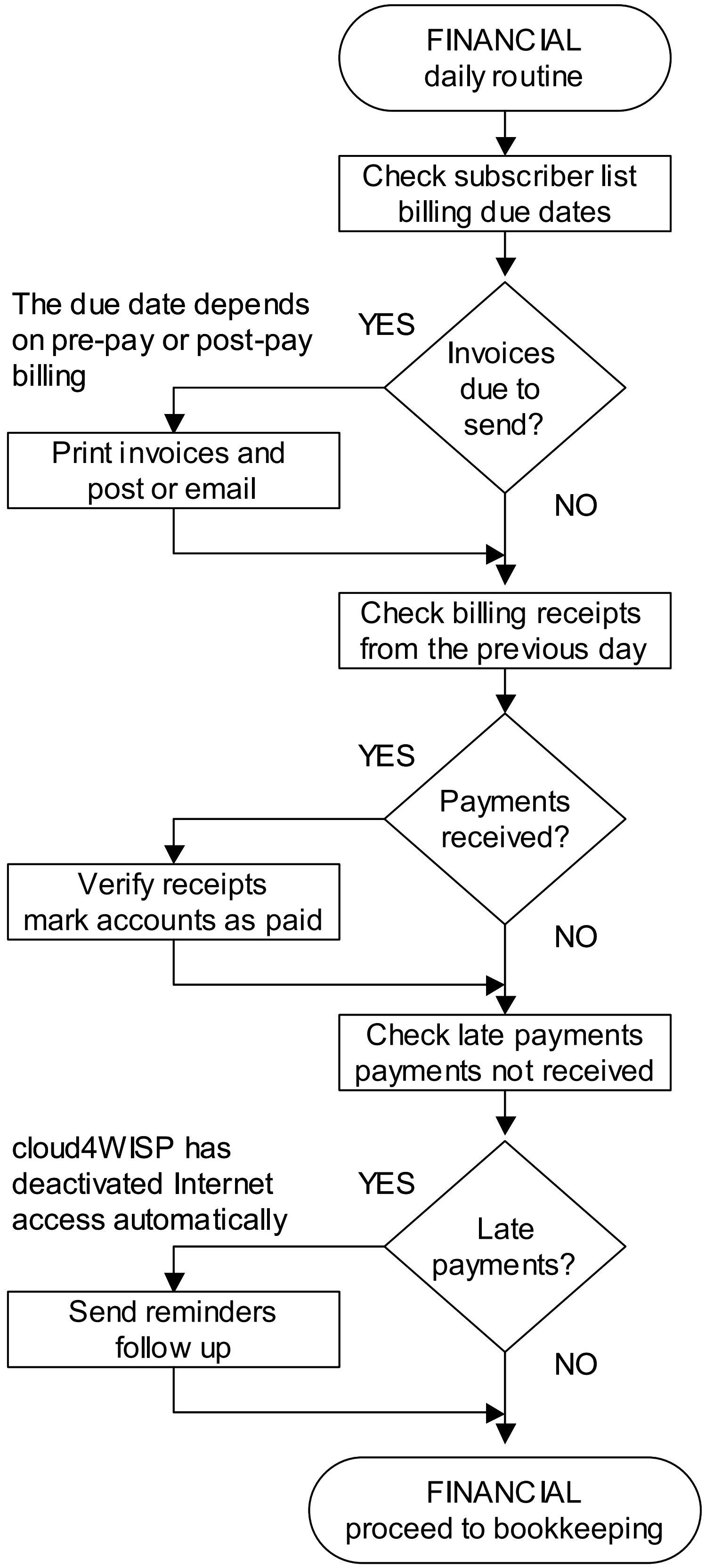


Figure 9.22.2. Flow diagram for the financial staff daily tasks.

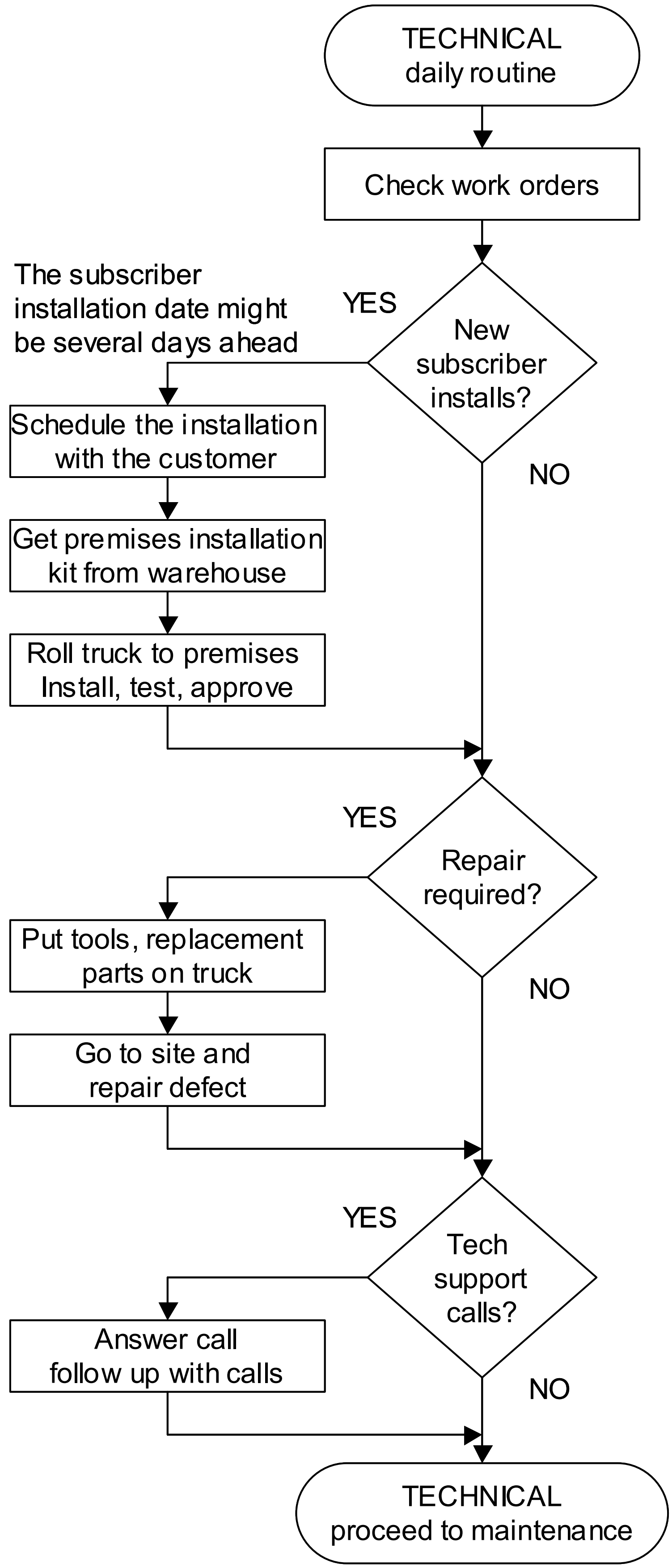


Figure 9.22.3. Flow diagram for the technical staff daily tasks.

Figure 9.22.4. Flow diagram for the support staff daily tasks.

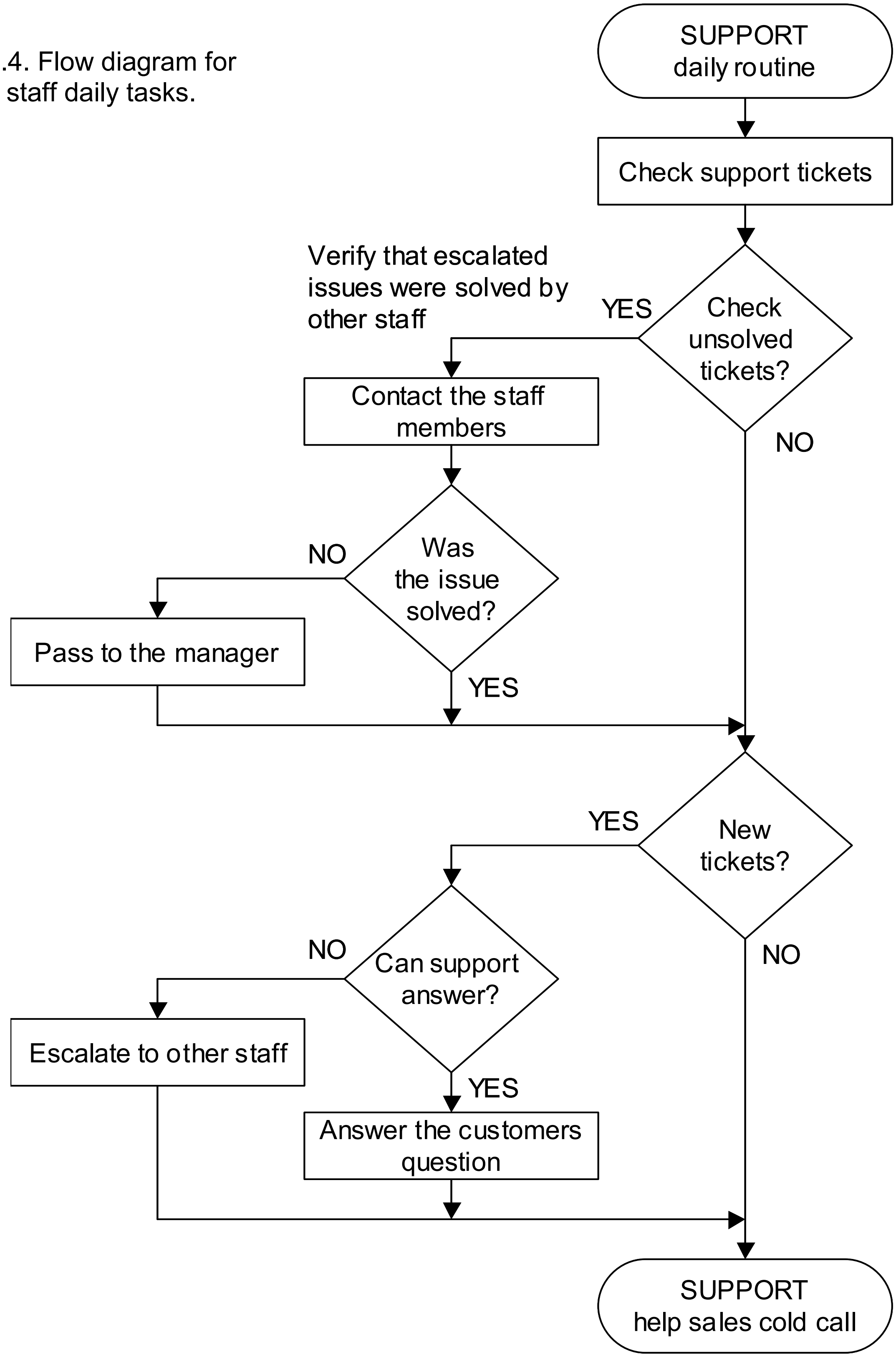
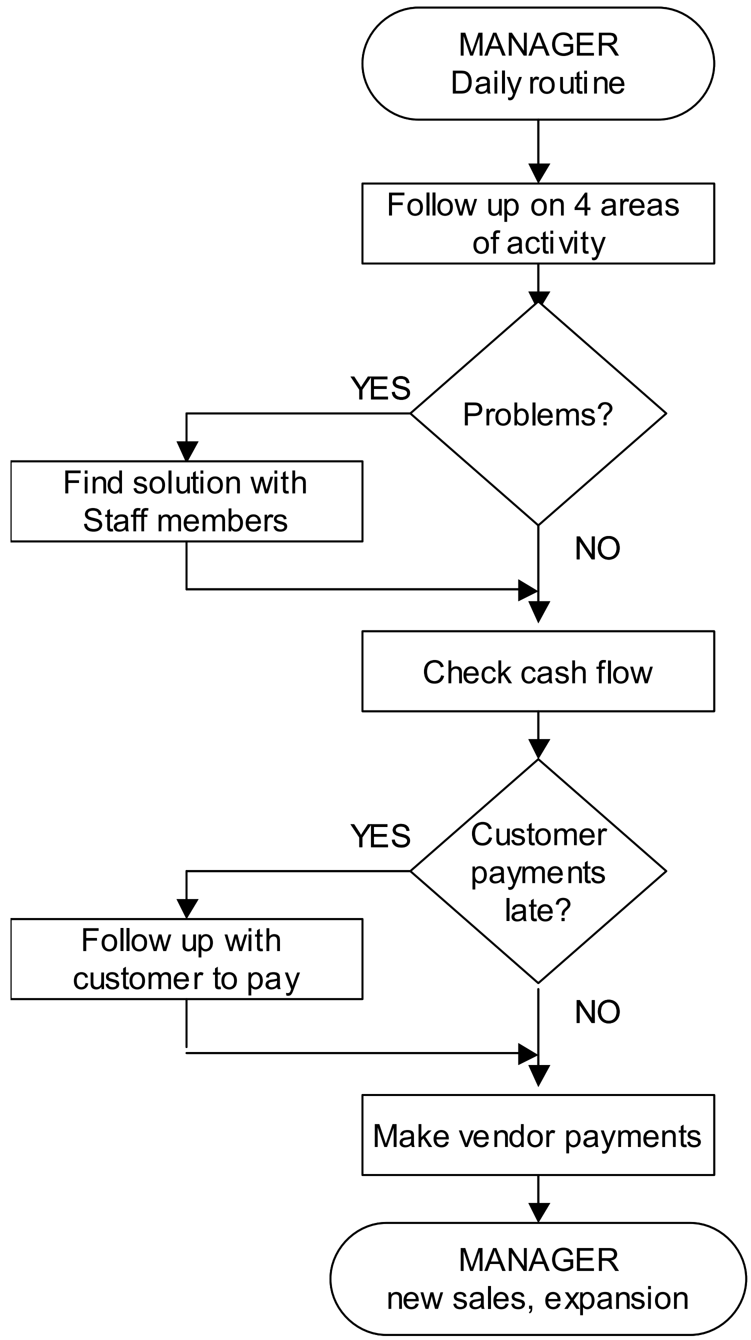


Figure 9.22.5. Flow diagram for the manager daily tasks.



Each WISP has tasks that are unique to that business. The WISP should elaborate flow diagrams that include the unique tasks. The preparation of flow diagrams is essential to support staff training and can be converted into an on-screen guide for each staff member to follow.

9.23. Summary

The key points or take-a-way's that a WISP entrepreneur should remember when planning to start a WISP business with a limited investment and a limited technical knowledge are listed below.

- Prepare a technical plan that is simple and within the entrepreneurs ability to manage.
- Define the business model, what are the services, how to provide the services, who are the customers, how to sell to the customers.
- First select the area of the target customers then plan the NOC and first PtMP tower.
- Plan the network design, the components required, the build out process, and identify who will help.
- Plan the tower design for a future transition to LEO satellite backhaul connections.
- Select WISP administration software that is simple to use, has the basic features required to manage the service, has access control router automation and has a very low cost per subscriber.
- Choose general-purpose routers that are configured for access control using command line scripts vs. routers designed for access control that work with specific software, have no programming and offer a higher level of performance.
- Carefully study the network build out to ensure that the most efficient path is planned before investing money to build the infrastructure.
- Become familiar with the software chosen to ensure that it is configured correctly.
- Prepare customer support and helpdesk for the customer’s view of the Internet service.
- When the serviced is established and customers are satisfied then begin planning the expansion of the service to new customers.

Glossary of acronyms

0-9

3G, 4G, 5G, mobile phone data connection types.

A

AAA; Authentication, Authorization and Accounting.

ADSL; Asynchronous Digital Subscriber Line.

API; Application Programming Interface.

APN; Access Point Name.

ARPU; Average Revenue per User.

AS; Application Server.

B

BNG; Broadband Network Gateway.

BSS; Business Support Systems.

C

CAGR; Compound Annual Growth Rate.

CAPEX; Capital Expenses.

CAT-n; Category n.

CATV; Cable TV.

CDMA; Code Division Multiplexing Access.

CDR; Charging Data Records.

CPE; Customer Premises Equipment.

CRM; Customer Relationship Management.

D

DDoS; Distributed Denial of Service.

DHCP; Dynamic Host Configuration Protocol.

DSL; Digital Subscriber Line.

E

EIRP; Effective Isotropic Radiated Power.

F

FTTH; Fiber to the Home.

FTTP; Fiber to the Premises.

FWA; Fixed Wireless Access.

G

GB; Gigabyte.

GE; Gigabit Ethernet.

GHz; Giga Hertz.

GSM; Global System for Mobile Communications.

H

HDTV; High Definition TV.

HSPA; High Speed Packet Access.

HSS; Home Subscriber Server.

HTTP; Hypertext Transport Protocol.

HW; Hardware.

I

IAB; Integrated Access and Backhaul.

IEEE; Institute of Electrical and Electronics Engineers.

IGW; Internet Gateway.

IP; Internet Protocol.

IPTV; IP Television.

IPvn; Internet Protocol version n.

ISDN; Integrated Services Digital Network.

ISP; Internet Service Provider.

ITU; International Telecommunication Network.

K

KPI; Key Performance Indicator.

L

LAN; Local Area Network.

LTE; Long Term Evolution.

M

MB; Mega-byte.

MBB; Mobile Broadband.

MHz; Mega Hertz.

MIMO; Multiple Input Multiple Output.

N

NAT; Network Address Translation.

NPV; Net Present Value.

O

OPEX; Operational Expenses.

OSS; Operations Support System.

P

PDN; Packet Data Network.

PoP; Wholesale telecom provider Point of Presence

POTS; Plain Old Telephony Service.

PtMP; Point to Multi-Point wireless connection.

PtP; Point-to-Point wireless connection.

Q

QoS; Quality of Service.

R

RADIUS; Remote Authentication Dial-In User Service.

RAN; Radio Access Network.

RF; Radio Frequency.

RJ11; Registered Jack 11.

RTP; Real Time Protocol.

RTT; Round Trip Time.

S

SDTV; Standard Definition TV.

SIP; Session Initiation Protocol.

SLA; Service-Level Agreement.

SME; Small and Medium-sized Enterprise.

SNR; Signal to Noise Ratio.

SPID; Service Profile Identifier.

STB; Set Top Box.

SW; Software.

T

TCP/IP; Transport Control Protocol /Internet Protocol.

TDD; Time Division Duplex.

TV; Television.

UL; Uplink.

USD; US dollars.

W

WAN; Wide Area Network.

WISP; Wireless Internet Service Provider.

X

XML; Extensible Mark-up Language.

Product suppliers for WISP’s

Lists of suppliers and manufacturers are included to assist WISP with the location of components to build and operate WISP networks. Most suppliers and manufacturers that are listed are located in the USA and the list is not exhaustive. Each country will have specialized WISP product distributors. Some of the products listed here are available globally.

WISP and ISP product distributors

ISPsupplies: https://www.ispsupplies.com/brands

Baltic Networks: https://www.balticnetworks.com/manufacturers

DoubleRadius, Inc.: https://www.doubleradius.com/brands

Winncom Technologies: https://www.winncom.com/en/products/manufacturers

Flytec Computers Inc: https://www.flyteccomputers.com/

Cayman Wireless: https://www.caymanwireless.com/

CTIconnect: https://www.cticonnect.com/

Last Mile Gear: https://www.lastmilegear.com/

Multilink Solutions Inc: https://multilink.us/

rOc-nOc: https://www.roc-noc.com/home.php

Streakwave: https://www.streakwave.com

SWG Inc: https://swginc.com

TESSCO Technologies, Inc: https://www.tessco.com

WAV, LLC: https://www.wavonline.com

WLANmall: https://www.wlanmall.com

Router product manufacturers for access control

Mikrotik: https://mikrotik.com/

Cisco: https://www.cisco.com/

Easywisp: http://www.easywisp.com

Tower power systems

Tycon: https://www.tyconsystems.com/Tycon-Solar_c_12.html

PtMP and PtP wireless product manufacturers

Cambium: https://www.cambiumnetworks.com/

Ubiquiti Air: https://www.ui.com/

Mimosa: https://mimosa.co/

Mikrotik: https://mikrotik.com/

Proxim: https://www.proxim.com/en-us/

Ligowave: https://www.ligowave.com/

Radwin: https://www.radwin.com/ptp-radwin-2000/

Ignitenet: https://www.ignitenet.com/wireless-backhaul/

WISP billing (some include CRM)

Iea: http://www.iea-software.com/products/emerald5.cfm

Ispbilling: https://ispbilling.com/

Visp: https://visp.net/

Billmax: https://www.billmax.com/what-problems-we-solve/

Aradial: https://www.aradial.com/

Onebillsoftware: https://www.onebillsoftware.com/network-broadband/

Wisplab: https://www.wisplab.it/?lang=en

Activeprism: https://www.activeprism.net/isp.html

Antamedia: https://www.antamedia.com/isp-billing/

Ispcube: https://www.ispcube.com/en/

easyWISP: http://www.easyWISP.com

Easywisp: http://www.easywisp.com

Iconwave: https://www.iconwavetech.com/telecom-broadband-billing-software

Network monitoring and management

Openwisp: https://openwisp.org/whatis.html

Zabbix: https://www.zabbix.com/

Auvik: https://www.auvik.com/

Sonar: https://www.sonar.software/wisp

Nagios: https://www.nagios.org/

Logicmonitor: https://www.logicmonitor.com/

Netelastic: https://netelastic.com/elastic-solutions-home/wisp/

Preseem: https://preseem.com/wisp-bandwidth-management/

Iwisp: https://www.iwisp.gr/

Billing with network monitoring and management (some with CRM)

Freeside: http://freeside.biz/freeside/

Ubiquiti: https://www.ui.com/uisp/

Powercode: https://powercode.com/features/

Azotel: http://www.azotel.com/

Swiftfox: https://swiftfox.net/

My-wifi: https://www.mywifiservice.com/en/software/WISP

Splynx: https://splynx.com/

Wispcontrol: https://wispcontrol.com/en/

Subscriber acquisition

Ready: https://www.ready.net

RADIUS for authentication

DMA: http://www.dmasoftlab.com/

Jumpcloud: https://jumpcloud.com

Cloudradius: https://www.cloudradius.com/

Radiusaas: https://www.radius-as-a-service.com/

Freeradius: https://freeradius.org/

Tekradius: https://www.kaplansoft.com/TekRADIUS/

Radiusgnu: http://www.gnu.org/software/radius/

Aradial: https://www.aradial.com/

Support tickets (part of the CRM system)

Osticket: https://osticket.com/

Zendesk: https://www.zendesk.com/

Mobile broadband hotspot software and hardware

Hotspotexpress: http://hotspotexpress.in/service_delivery/isp.html

Guest internet: http://www.guest-internet.com

Customer service

Calix: https://www.calix.com/solutions/service-providers/wisps.html

Third party services that WISP's resell

Wisptv tv: https://wisptv.com/

Nextiva phones: https://www.nextiva.com/

Eagleeye security: https://eagleeyepro.com/

WISP trade organizations

WISPA USA: https://www.wispa.org/

WISPA UK: https://www.ukwispa.org/

ISP UK: https://www.ispa.org.uk/about-us/organisation/

WISP annual conferences and expos in the USA

Wispapalooza: https://preseem.com/wispapalooza/

Wisp: https://wispaevents.org/

FCC filing for WISP's

FCC FORM 477: https://www.fcc.gov/general/broadband-deployment-data-fcc-form-477

FCC FORM 477: https://form477mod-ui.fcc.gov/home

Reporting: https://www.cooperative-networks.com/how-to-report-477-data-to-the-fcc/

LEO satellite Internet providers

Kepler Communications: https://kepler.space/

SpaceX Starlink: https://www.starlink.com/

Boeing: https://www.boeing.com/space/boeing-satellite-family/

Airbus Defence and Space: https://airbusus.com/leo-constellations/

Amazon Kuiper: no website

Oneweb: https://oneweb.net/

Telesat: https://www.telesat.com/leo-satellites/

Geo-stationary satellite Internet Providers

Hughes: https://internet.hughesnet.com/

Viasat: https://www.viasat.com/

Echostar: https://www.echostar.com/

FIGURES

TABLES

About the Author

John D. Barker is a member of the Institute of Electrical and Electronic Engineers (MIEEE) and is a computer engineer who has over 40 years of experience with the computer and network product manufacturing industry and with the development of software and services for computer network applications. The author established a company to manufacture Ethernet interfaces for PC computers in the early 80's and was the first customer of Intel Ethernet chips. Later while working for the consulting firm Booz-Allen and Hamilton the author advised both cable TV companies and telecom companies how to transition into the Internet service provider business segment. Following this period the author worked for Compaq Computer and Hewlett-Packard as Director of Network Services, with work that included advising Internet Service providers and Wireless Internet Service Providers about the applications of networking technologies and assisting them with network design projects. In 2005 the author established a company together with partners to develop and manufacture hardware and software products for both mobile broadband and fixed broadband service providers, and continues with this project to the present date.

The author graduated from Leeds Municipal University, UK, in Electronic Engineering and was awarded M.Sc. and Ph.D. degrees in Electronic Engineering and Computer Science from the Cranfield University, UK.

Contact the author at the email address:
john@fire4.com