rapiersystems
We Live Wireless!

Building a Metropolitan Area Network with Wireless

Introduction

This document is designed to illustrate the principles behind building a Metropolitan Area Networks using Wireless technology. It's important to note that this technique and model is almost infinitely scalable, being suitable for smaller areas such as business parks or college campus environments, and can be scaled in the other direction and taken wider across entire counties or even countries. The rules and methodologies are the same. The only difference is the wireless technology deployed.

Applications and justifications for Metropolitan Area Wireless Networks

Financial

For most of our customers, the primary driver for looking at these technologies are initially financial. A typical new client has needed telecommunications infrastructure and made an inquiry of, one of the large national Telcos. If there is no appropriate infrastructure in the area, the cost of building out the Telco's network to a new area will be borne by the client, usually amortized across a 3 year contract, in a similar way to the way the mobile carriers cover the cost of £600 smartphone handset over the life of a mobile contract.

Unfortunately, the costs of fibre digs and infrastructure additions are high, and the client is often faced with an eye wateringly high quotation for a service that is business critical to that location and a vastly extended 'go-live' date as the carrier organises not only the logistics of road digging crews, but also the wayleaves and permissions from local government required to dig up a public street. Most antennas are classed as 'de-minimis' by local planning authorities and therefore don't permission.

A solution based on radio technology is often a much cheaper solution, requiring initial installation/survey fees and an annual maintenance contract.

Speed of Implementation

Wireless links can be introduced into a customer's network quickly and with minimal fuss and disruption to normal business operations.

Most building to building systems simply require permission to use the roof or another area of the building that has line of sight to the other end of the link, a stable power supply, with sufficient capacity to run the equipment and a way to access the core network, usually via Ethernet cabling or a fibre optic connection.

This means that in the right circumstances, a radio link can be planned and implemented in days rather than months.

Flexibility

Most data based services can be carried over wireless network systems, provided they are correctly planned and dimensioned. Most clients initially think of data services, for provision of Internet access or site to site communications, but Voice Over IP (VOIP) telephony systems can radically reduce inter-site communications costs.

Other services that can be integrated include;

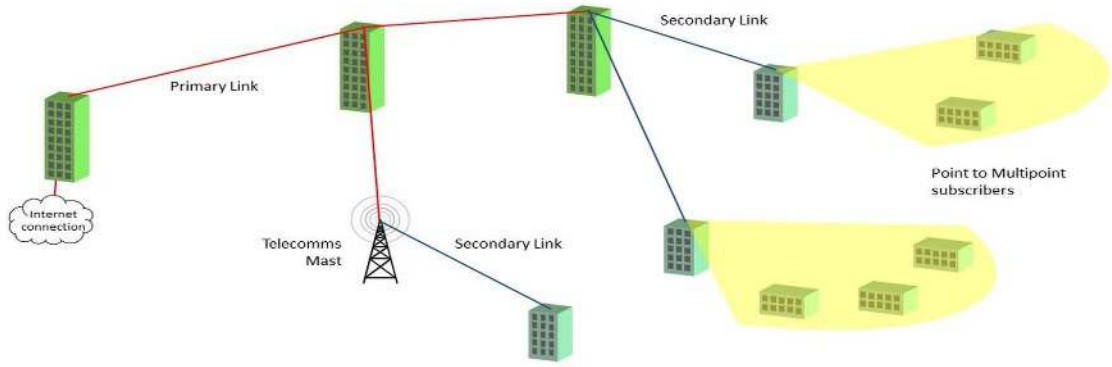
- CCTV Security systems.
- Concierge Systems, incorporating video entry systems, door buzzers, help points and remote door latches.
- Automatic Number Plate Recognition Systems (ANPR) for parking enforcement/Car park entry control, automatic barriers and traffic speed measurement.
- High Quality Video for Post Production in TV Studios or Telemedicine
- Public Wi-Fi hotspots, internal or external
- Multiple 'Virtual Networks' for Multi-Tenant dwellings or offices.
- Process control/monitoring systems in an industrial environment.

The high speed of deployment for wireless technology also adds to the flexibility, with temporary installations for special events and clients that only occupy office space for short times, for instance, in a business incubator environment.

Another advantage of wireless over fixed infrastructure is that it can be relocated, so if business circumstances dictate a move, the hardware can often be redeployed.

rapiersystems
We Live Wireless!

Building a Metropolitan Area Network with Wireless



The diagram above shows a typical configuration for Metropolitan Area Network. The design is modular, allowing scaling of the network over larger areas with minimal disruption to network operations. The various elements depicted break down as follows.

Internet Connection/Data Centre

This is the 'hub' of the network, providing access to the services that the users on the network require. Typically, in a wireless broadband network, this is a high speed fibre connection to the internet, with firewalling and redundant equipment for a larger network. Multiple lines to the Internet from multiple providers can be implemented if redundancy is a desirable requirement.

In a corporate environment, such as local government network, this would be the central data centre, housing the servers and services that the users on the network require.

Primary Links

The Primary links are the 'backbone' of a Metropolitan Area Network. They provide high speed, (typically Gigabit) point to point data services between key locations in the network. These are mission critical for the operation of the network, and as such, must be solid and reliable, with a secure power supply, careful installation and planning. It is not unusual for the backbone network to be built with multiple paths and redundant links to ensure data integrity in the event of a failure. Where direct line of sight is not available, these point to point links can be 'daisy chained' using intervening roof areas or communications towers.

Secondary Links

Secondary links provide service from the main network nodes to local distribution points or key customers with high bandwidth requirements. Speeds are normally measured in the hundreds of Megabits per second, depending on the application.

Local Distribution

Local distribution can take several forms:

Point to Multipoint Sectors

Point to Multipoint Sectors are typically deployed in commercial Wireless Broadband networks. A local node point is fitted with a 'sector' antenna, which distributes a radio signal over a distance of up to 2km in a 90 or 60 degree arc. Subscribers within this sector are fitted with a small receiving antenna and get a share of the bandwidth available. Careful planning and management of available bandwidth is required to ensure that subscribers get the service to which they are contractually entitled.

In-building Distribution

A multi-tenant unit can be fed via either a point to point link, or a point to multipoint, depending on speeds, contention ratios and services required. Once the radio on the roof is cabled internally, the services can be delivered either over standard Ethernet cabling, or via a wireless network.

An internal wireless network is a good choice for a multi-tenant business unit as with a little careful planning, coverage can be achieve across the building. Virtual wireless networks can then be set up, with each client inside the building having their own credentials and service levels.

Outdoor Wi-Fi Nodes

As with the above, Outdoor Wi-Fi nodes can be fed via either a point to point link, or a point to multipoint link. These usually use omnidirectional antenna, providing a small 'bubble' of connectivity in environments such as tourist spots, cafés or campsites. Outdoor Wi-Fi nodes can be clustered together in these environments, providing small access networks.

rapiersystems
We Live Wireless!

Building a Metropolitan Area Network with Wireless

Technologies Involved

There are 3 main technologies involved in the building of these networks, each with its own particular strengths and parts to play in an integrated system.

Licenced Microwave

Licenced microwave is the ideal technology for long primary backbone links. Distances in the tens of kilometres are possible. This is the technology upon which 90% of the cellular networks are based.

These systems provide high capacity Point to Point links, with very predictable throughputs. These systems require clear, unobstructed line of sight.

Licenced Microwave systems require a specific operator's licence obtained from OFCOM, the UK body who regulate the wireless frequency airspace. OFCOM will allocate the frequency to be used between two points, ensuring there can be no radio interference that may affect the signal. An annual fee is payable for this peace of mind.

Light Licenced Radio

Light Licenced Systems require a registering with OFCOM, for a nominal annual fee. The frequencies are not policed by the radio authorities.

Light Licenced radios are available in both Point to Point and Point to Multipoint varieties, with distances and line of sight requirements based on the frequency used.

Light Licenced radio systems can be used for short distance, high capacity, primary backbone links at a lower price point than the licenced microwave alternative.

Alternatively, light licenced Point to Multipoint radio systems can be deployed to provide service to multiple clients in a defined geographic area, each taking a defined share of the available bandwidth. These systems are optimised for wireless broadband delivery.

Wi-Fi

Modern Wi-Fi systems are probably the most commonly encountered radio systems, with consumer devices such as mobile phones, laptops, tablets and even TVs shipping with an integral radio.

Modern Wi-Fi is optimised as a short distance access medium and the term is almost interchangeable with broadband delivery in the domestic environment.

Because of this proliferation and the fact that the frequencies are not only unlicensed, but also shared with other devices such as wireless telephones, careful planning is required to fully optimise the coverage across a building in a professional installation.

High end Wi-Fi systems, typically incorporate some kind of controller functionality, be it local or 'cloud based' to proactively manage the radio spectrum, optimise performance and mitigate interference.

rapiersystems
We Live Wireless!

Building a Metropolitan Area Network with Wireless

Challenges

There are a number of challenges inherent in building a network of this type. This section is intended to address these issues. Careful network planning, equipment selection and professional implementation are key to ensuring a Metropolitan Area Network is safe, secure and reliable.

Data Security

Data security is one the most common concerns about wireless technology. These concerns were founded in the early implementations of Wi-Fi networks that used the Wired Equivalent Privacy (WEP) encryption standard. This was notoriously weak and was able to be cracked in minutes using standard laptop hardware. Modern Wi-Fi systems use a system called Wi-Fi Protected Access (WPA2) as a bare minimum. This uses a 256bit key and is considerably more difficult to hack.

Good practice is key to data security. In a corporate environment, using a central authentication server to manage user sessions provided greater security. Managed Wi-Fi systems can provide protection against unauthorised access by identifying 'rogue devices' and blocking them.

In an open environment, where user access needs to be open, security should be implemented at the session level.

Most Point to Point and Point to Multipoint systems use proprietary coding techniques in addition to high levels of data encryption, making them exceptionally difficult to intercept. For these systems, in most cases, it is easier for unauthorised access to be gained at the Ethernet level, by accessing the rooftop sites and rerouting cables than accessing the wireless element, so careful base station design and security is key.

Compliance

Recent EU Directives make clear the importance of protecting and recording certain user data; this places a burden of responsibility on businesses that provide public Wi-Fi.

There are three important aspects to consider:

Data Retention

Under the Data Retention (EC Directive) Regulations 2009 and the January 2004 the Code of Practice certain types of data are required to be retained to identify end users accessing the Internet. This includes traffic and location data (to help trace the source of a communication).

Examples of relevant data include: –

- User ID; name and address; date and time of login and log off
- IP address allocated to a user; MAC Address, originator of the communication;
- Internet Service used (HTTP, POP, IMAP, SKYPE etc.).

The Home Office expects such data to be retained for a minimum of 12 months.

Copyright

The Digital Economy Bill became law in June 2010; it targets online copyright infringement, including the illegal downloading of copyrighted material and illegal file sharing. It places obligations on providers of public Internet access to keep end user records to assist copyright owners in identifying breaches and taking action.

Data Protection

Under the Data Protection Act 1998 any user of Internet access in a public place is entitled to request at any time details of his/her personal information. Failure to securely maintain and make available this data is an offence and may lead to the imposition of fines by the Information Commissioner.

Unless you get explicit positive affirmation from the user (tick box or via T&Cs) you cannot use this data for marketing purposes and it can only be disclosed to appropriate authorities.

User session management

In a public Wi-Fi network, management of the users is a key element. Simply providing an open network and letting the users fight for access is likely to result in a poor user experience, and falls short of Compliance regulation.

A properly managed network will control the user's log on and log off 'journey', implementing sensible timeouts in the event of the user leaving the physical location and record the information necessary for compliance purposes. In addition, this can provide bandwidth shaping, allowing users only to consume the bandwidth to which they are entitled.

rapiersystems
We Live Wireless!

Building a Metropolitan Area Network with Wireless

Bandwidth Management/Network Scaling

Carefully dimensioning the information flow across the network is key to good operation and high levels of user satisfaction. A careful analysis of perceived traffic flows, ensuring that critical Primary backbone links, Internet feeds and access networks do not become saturated will go a long way towards this.

When serving end-users, an idea of the applications used and required contention ratios is exceptionally useful. The use of traffic shaping and content management are useful tools to maintain stability. As an example, a rural network with a slow connection to the Internet will run exceptionally poorly if the users are allowed to access video streaming services such as YouTube, iPlayer or Netflix, something a lot of Wi-Fi enabled Caravan site owners will attest to!

Again, equipment selection is a key part to maintaining long term stability. Choosing products that can be upgraded via software key to cope with increased future demand is a good strategy.

Implementation

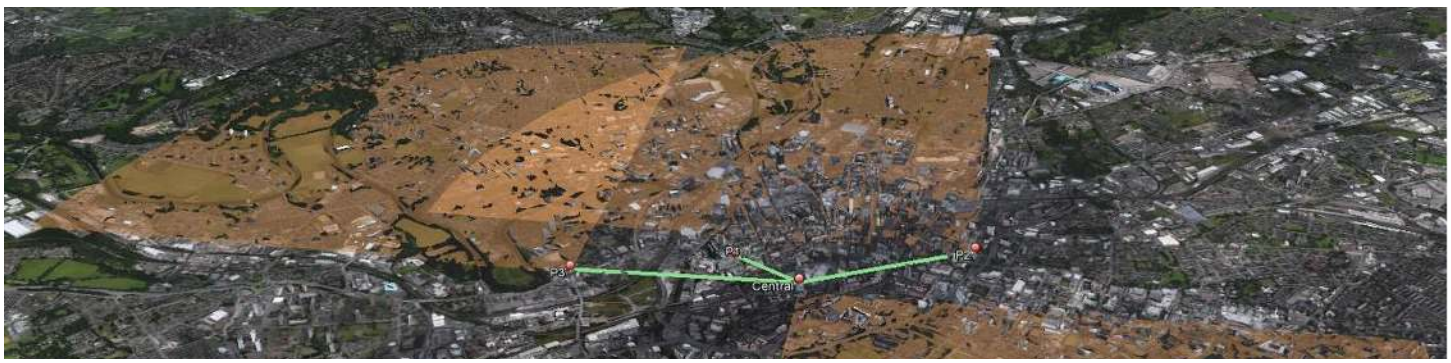
To ensure a successful implementation of any wireless network, there are several steps. Of all these steps, regardless of the technology being deployed, planning is the most crucial.

Planning

Planning should always start with a careful analysis of user requirements, applications and geographic spread. Obviously, this varies from network to network, with Wi-Fi and city wide deployments having different requirements. Planning will identify the start and end points of data flows and define the bandwidth required to serve these users.

Wide area planning

In the case of a Metropolitan Area Network, the available assets and geography can then be studied and modelled to define the initial network design and shape the survey parameters. This will enable visualisation of the coverage area and help dimension the project accurately.



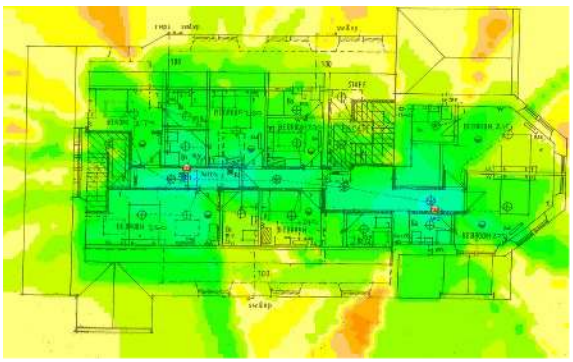
One of the most crucial elements is the site acquisition process. With the rise of the mobile networks, rooftops are recognised as assets by most building owners. Careful negotiation can usually get access to appropriate rooftops, but it is unwise to proceed with other elements of network build until these permissions are firmed up.

Wi-Fi Planning

In the case of a local Wi-Fi network, the planning process is similar. Building interiors can be modelled from scaled architects plans, supplemented with construction information. The result is a predicted coverage plan and equipment list.

In most cases, these virtual survey tools provide a good indication as to the final 'look and feel' of the network, also giving a good approximation of build costs.

Virtual surveys, should NEVER, however, be taken as a final design. There are far too many factors in the real world that can effect network performance and these cannot always be modelled. Their purpose is to provide a starting point for the physical survey.



rapiersystems
We Live Wireless!

Building a Metropolitan Area Network with Wireless

Survey

Once sites have been acquired and the modelling completed, the project moves to site survey stage. The survey has several purposes:

Verification of Calculated results

The first part of the survey is to verify that the planned network is viable in the real world. Factors such as tree cover, new building developments not identified in mapping can affect the networking topology. If the direct path is not viable, intervening structures such as alternate rooftops and telecommunications towers can be identified and information passed back to the planners for further study.

Line of sight links are simply verified with binoculars and evidence gathered with DSLR cameras equipped with telephoto lenses. Wi-Fi and non-line of sight networks are verified by real work testing, with equipment temporarily deployed and real world signal measurements taken to ensure performance is as planned.

Services Planning

Once the radio path is identified, the physical part of the installation is documented. Mounting locations for the radio equipment and any associated indoor equipment are documented. Also the type of supporting hardware is identified, together with data cable runs and identification of power supply locations, with recommendations for any addition capacity required.

Definition of access requirements

An important part of the survey is the identification of how the unit will be installed and serviced, whether it be on ladders, climbing to the location or via Mobile Elevated Work Platform (MEWP).

Health and Safety Audit

Finally, a health and safety audit is performed and fully documented, to ensure the safety of users, installation and service personnel and the general public.

Report

All of the above items are written up into a full site survey report. This forms a 'blueprint' for the installation teams and forms an integral part of the Risk Assessment and Method Statement (RAMS) documentation. This attention to detail ensures a successful, safe installation which meets the customers' requirements.

Installation

If the planning and survey process have been completed and documented correctly, installation is a relatively straightforward process.

The engineers have a clear work instruction, are prepared for site conditions and have the appropriate equipment, tools and mounting hardware.

Once the equipment is installed, cabling installed and secured and all power supplies instated, the radios are aligned to the planned signal levels.

Operational factors such as signal level and throughput are recorded and the installation is documented and photographed. This information forms the basis of the post-installation documentation, crucial for support purposes. If appropriate, the systems are connected to network management systems and monitoring visibility verified with the networks operation centre (NOC).

The equipment can then be brought into service and handed over to the customer.

rapiersystems
We Live Wireless!

Building a Metropolitan Area Network with Wireless

About Rapier Systems

Formed in 2003 Rapier has unrivalled expertise in the design, delivery and support of wireless (including WiFi) networks and systems; the company is a value added integrator of best-in-class wireless products.

Whether within or between buildings, upgrading or replacing existing networks, or designing and installing new wireless systems, Rapier's experience in environmental analysis and network design ensures complete coverage and optimal performance.

Rapier works with world leading wireless system vendors, including Ruckus, Alvarion, Airtight, Cambium/Motorola, Ceragon, SAF Technika and several more. The company has reached the highest level of accreditation with each of its partners and understands which vendor and product is best suited for each environment.

Rapier has grown dramatically on the back of a surge in demand for wireless networks, which it has designed and installed in a wide variety of challenging environments from colleges and oil rigs to business parks and theatres.

Rapier maintains Scotland's largest Wireless Network, covering Dundee City, Angus and Perth & Kinross Councils, which comprises around 250 sites.

The company has designed and delivered some of the most innovative wireless solutions in the UK, including the largest metropolitan area wireless network in Scotland and one of the largest county-wide wireless networks in England. Rapier delivered the 1st fully licensed Gigabit wireless link in the UK.

The company's headquarters is located in Fife, Scotland and it has offices in St Neots, Cambridgeshire, England.

Rapier has a UK wide customer base in sectors that include Local Government; Transport, Renewables, Oil and Gas, Retail and Leisure.

For further information please visit **www.rapiersystems.com**

Rapier Systems Limited
Ore Valley Business Centre, 93 Main Street, Lochgelly, Fife, KY5 9AF
Tel: 0845 299 6171 E: info@rapiersystems.com W: www.rapiersystems.com

Registered in England - Registration No 4821724