Andrew Saoulis
Andrew Saoulis works for Case Communications and has worked there since the early 1980's. He has designed computer networks for 35 years both in the UK and internationally, and is also responsible for guiding Case Communications product development. Previously Andrew worked for Racal-Milgo, Rank Xerox, Barclay Bank (Computer Centre), and the GPO (now BT).

1. INTRODUCTION

Thirty years ago how many Traffic Engineers could have imagined that as well as needing to learn about traffic systems, they would manager computer networks as well?

Making a decision over what type of network to implement is a difficult decision at the best of times, and with a slick salesmen and the large number of acronyms in the communications world it can be very confusing. How many times do we see customers purchase networks that are completely unsuitable from a very plausible and pleasant salesman?

Often there is no single technology to suit every scenario; for those that can afford to install fibre, it makes sense in the city centre but in the more remote areas where network points are spaced further apart it can be too costly to install fibre, meaning other solutions provide better options.

The decision on whether to use a Private or Public network is a decision largely dictated by the budget. When using a private network we may expect complete control of that network, but for a higher capital cost and lower operational cost. When using a public network we can expect a lower capital cost but greater operational costs. Budgets are a major consideration, a policy of 'Spend to Save' needs justification and faith that the capital investment is going to lead to savings, support for more services and greater reliability. Other considerations are the applications to be run over the network, are they bandwidth hungry or do they need low latency, what is the effect of the data getting corrupted and do we need error correction or do we need to simply get as much of the data through as possible and not worry about packet loss, such as sending video for example?

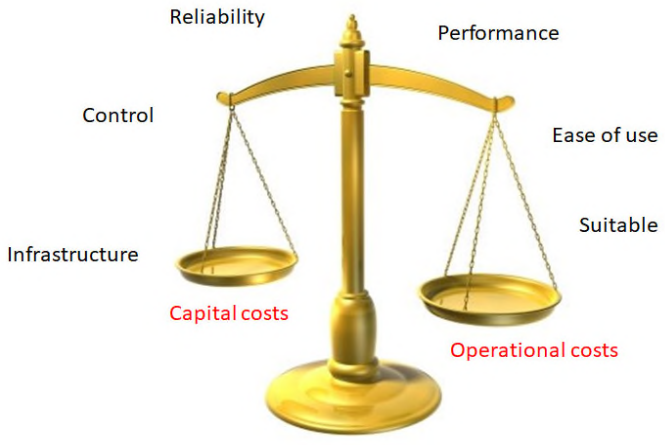
1.1 A BALANCING ACT

When selecting a network technology the traffic engineer has to perform a difficult balancing act.

The diagram to the right considers some of issues to be decided in balancing the network requirements.

If a 'Spend to Save Policy' can be implemented Capital Costs will be greater but savings can be made on Operational costs.

Support issues must also be considered how easy it to support the network is, how easy is the network to configure?



We also need to consider the type of traffic that is to be run over the network, for example do we need real time video and higher bandwidth up-stream, or do we only need UTMC Traffic and good data integrity but at a low data rate. The ideal is high bandwidth, with reliability and good data integrity (i.e. clean data with no data errors).

2. PUBLIC NETWORK TECHNOLOGIES

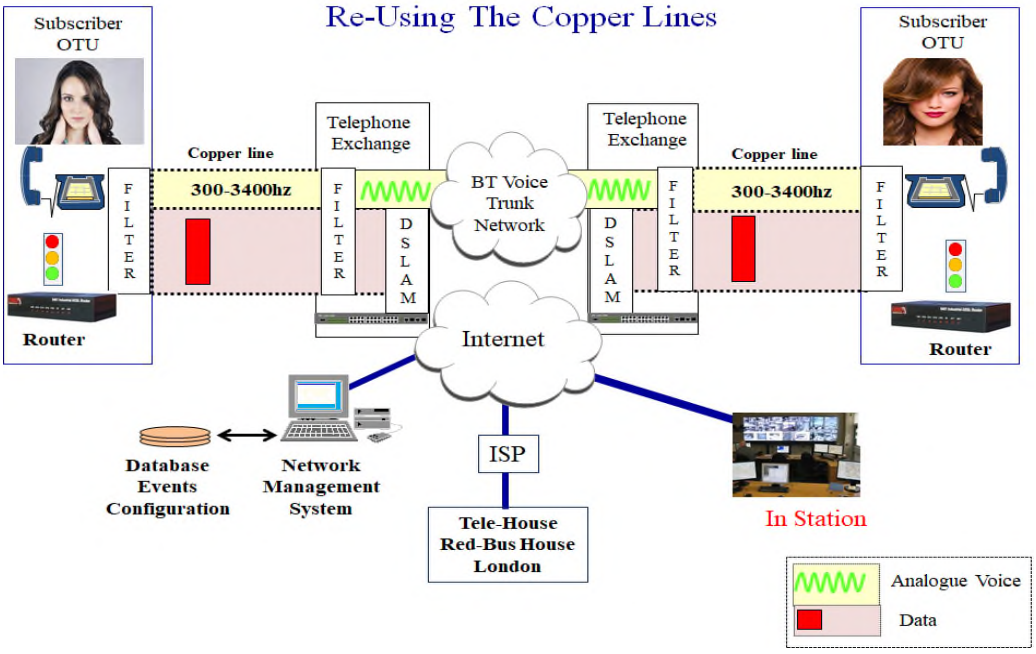
3.1 DSL NETWORKS - (Digital Subscriber Loop)

All DSL technologies use a local copper circuit between the subscriber (BT talk for customer) and the local Telephone Exchange. Typically these are copper but there are a few aluminium circuits in use which provide poor performance.

ADSL – stands for **A**symmetric **D**igital **S**ubscribers **L**oop which is a local Access Technology where we have no frequency restrictions on the copper circuits. ADSL uses a Filter to take the voice bandwidth out (300Hz to 3,400 Hz) allowing data to use the rest of the bandwidth. Asymmetric means the traffic going from the telephone exchange to the subscriber is greater than from the subscriber to the exchange. This is because most users want to surf the Internet and download rates are greater than upload rates. ADSL2+ has a maximum data rate of 24Mbps downstream and 2Mbps upstream. If your network Router and ISP are capable of supporting 'Annex M' then the upstream data rate can go to a maximum of 3Mbps at the cost of some downstream bandwidth.

The maximum range for ADSL is around 6km depending on the quality of the copper and the closer you are to the exchange the better the quality of copper, the higher the data rate you will obtain.

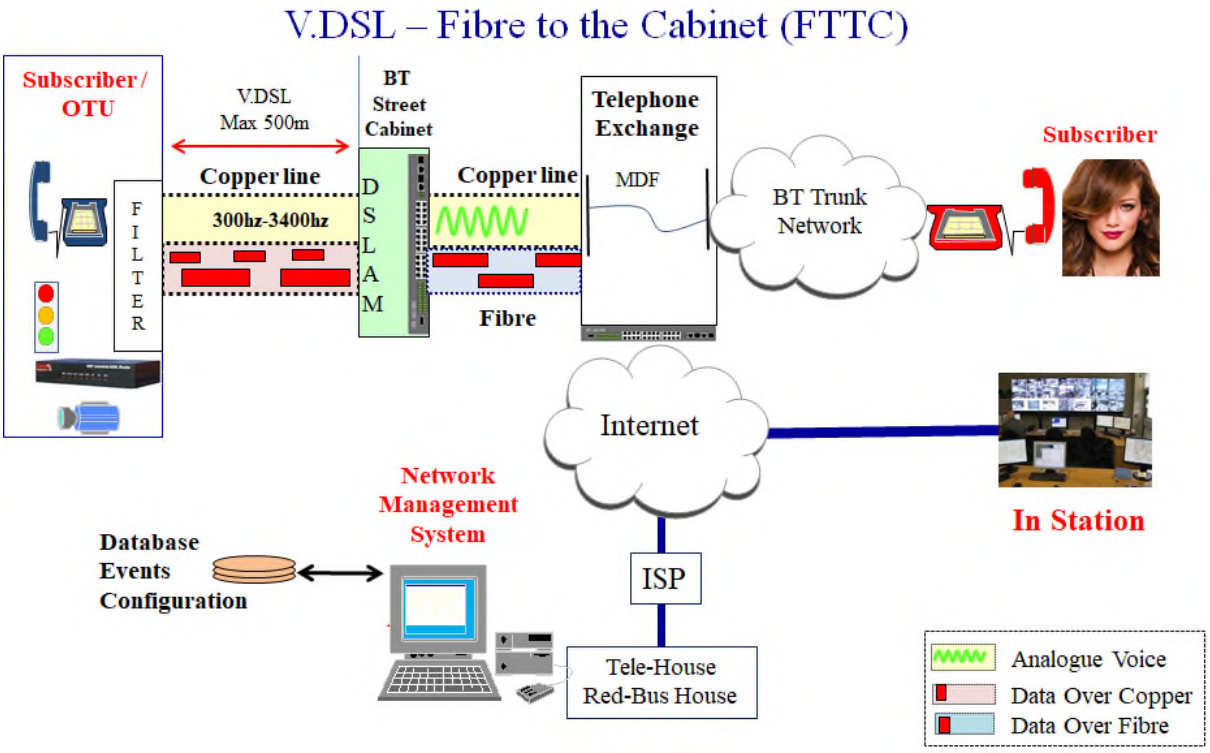
One of the benefits of using a public network is that your equipment can be monitored by a third party such as Case Communications. Case can tell you the status of your network and connect to your network device to make changes on your behalf. The diagram below depicts a typical ADSL connection.



V.DSL (FTTC (Fibre to the cabinet))

Very High Speed Digital Subscriber Loop – This is a short range technology (operating up to 500m) which BT currently sell as 'Fibre'. In fact it's not really fibre, but 'Fibre To The Cabinet' (FTTC). BT currently offer two rates for FTTC, the first being 10Mbps upstream / 40Mbps downstream, and the second 20Mbps upstream / 80Mbps downstream. This makes FTTC suitable for running real time video and other applications requiring higher upstream bandwidth. V.DSL is similar to ADSL using a filter to take the 300Hz to 3,400 Hz voice band out of the data path, allowing data to use the rest of the bandwidth.

The diagram below shows a V.DSL Connection. Notice the local BT Cabinet in the street contains the DSLAM and splits the voice and data. The voice goes to the exchange via copper circuit while the data goes via Fibre. The diagram below depicts a V.DSL (FTTC) Network Connection.



FTTP- (FIBRE TO THE PREMISES)

Fibre to the premises is offered by the likes of Virgin Media (Really NTL, who pay Virgin to use their brand) and they advertise data rates of up to 300Mbps into their network. However this is not available everywhere, and once your data gets into the local exchange, the backhaul to the Internet needs to be sufficient to support all the incoming users. This is not something a customer could easily find out.

BT have announced FTTP (as of July 2017) and to start with they will be offering the same data rates as their FTTC service, i.e. 10 /40Mbps and 20/80Mbps. BT have said they will increase these rates in time, but it's a very new service it maybe some time before we see rates increase.

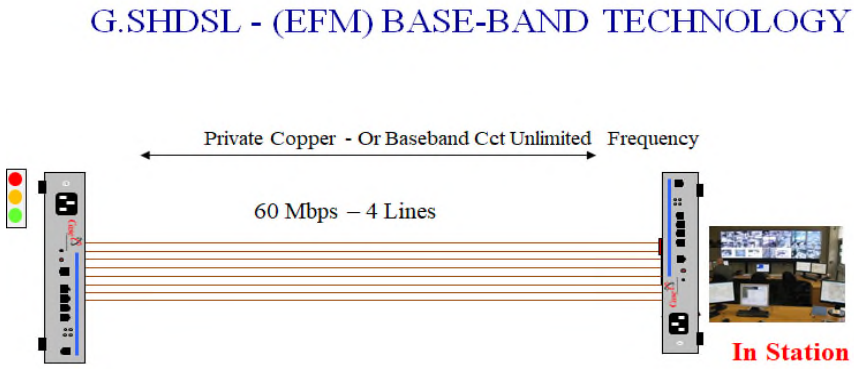
Pros and Cons of using a DSL Network	
Pros	**Cons**
Low capex Costs	Designed for download not uploading
Relatively low operational costs	Upstream better on V.DSL than ADSL
As the equipment is on a public network your equipment provider can manage the equipment for you.	Runs over Public network which you have no control over. You may only want the data to travel a short distance, but the data could travel some distance to London (Tele-House / RedBus-House) and back.
Available almost everywhere	BT say if you need a reliable network don't use the Internet but use BT 21CN Network
	It's necessary to use complex security to protect your data
	Occasional lock ups by BT DSLAM means your routers need to check the health of the network and perform a restart or go to 4G if necessary

G.SHDSL – G.SYMMETRICAL DSL –ALSO CALLED ETHERNET FIRST MILE (EFM)

G.SHDSL is a technology that does not filter out voice but uses the whole of the copper circuit for data, so any telephony required has to be VoiP. As the title 'Symmetrical' suggests we have the same upstream and downstream bandwidth.

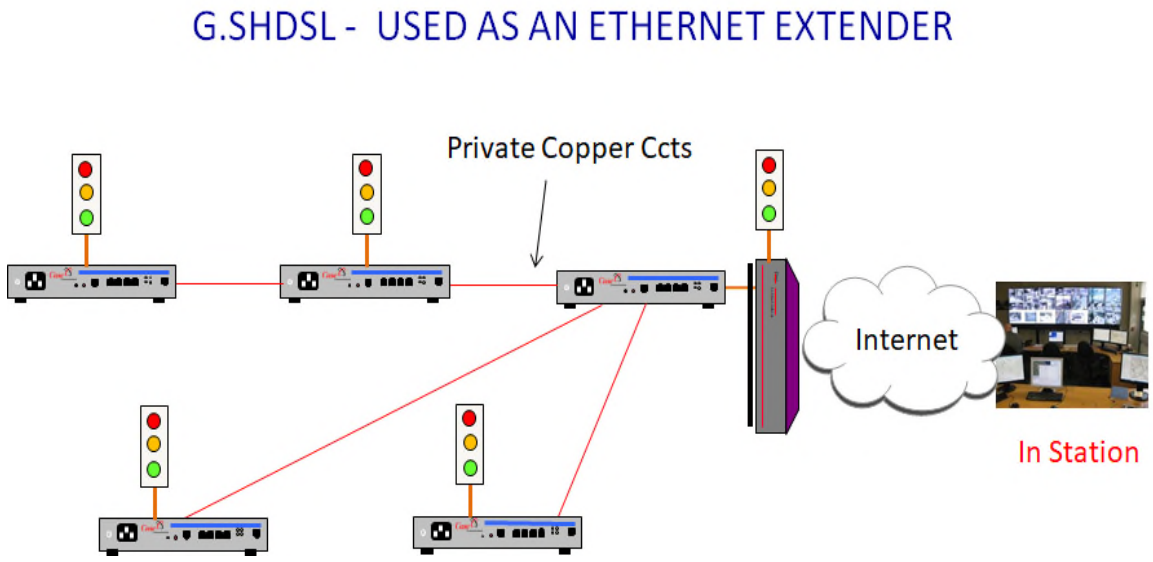
The latest standard in G.SHDSL is G.SHDSLbis which gives maximum data rates of 15.296Mbps each way on a single pair of copper wires (in the field the actual data rates depends on the quality of the copper circuit and distance of the line). Case G.SHDSL products can bond up to 4 circuits providing 60Mbps each way, more than enough for Video and real time applications.

A typical point to point G.SHDSL link bonding 4 pairs can be seen in the diagram below



G.SHDSL is also used to extend Ethernet

However to operate this kind of technology requires a dedicated copper circuit between two subscribers operating within the same telephone exchange. These circuits were called Baseband Premier and Baseband Standard. BT Wholesale hates selling these circuits and won't offer an SLA, and if you ask your BT salesman for a quote the chances are they won't know what you're talking about. Therefore its unlikely you will continue to use this technology on BT Wholesale circuits, but you can use them on your own private copper circuits.



Many authorities have their own copper, and G.SHDSL / EFM technology can also be used as an Ethernet Extender. The diagram above shows O.T.U's being connected to a router at the head site and being fed by G.SHDSL products, running in 'Daisy Chain' mode and 'Multi-Drop' mode. These products can also operate using Fibre making an upgrade from copper to fibre very easy.

3.2 MOBILE NETWORKS

Almost everyone (89.9 Million subscribers in 2015) has a mobile phone these days and the use of a mobile network for data communications is common place. Mobile network Base Stations (Up to 52,000 in the UK) build radio cells with a typical range of up to 35Km, using frequencies of 1800 MHz and 900 MHz.

Maximum Data Rates in mobile networks

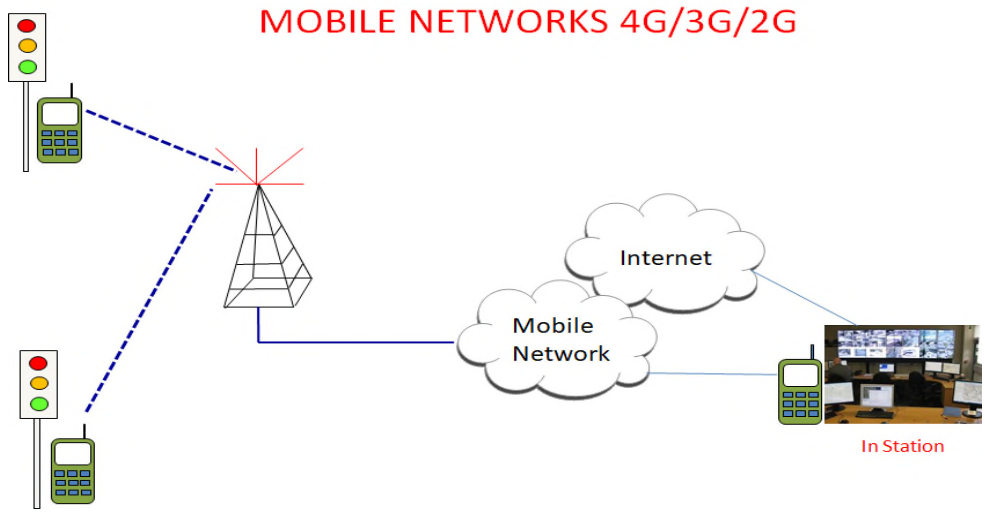
When discussing mobile throughput, there is a distinction between the peak data rate of the physical layer, the theoretical maximum data throughput and typical throughput.

The peak rate is the net bit rate provided by the physical layer in the fastest transmission mode (i.e. using the fastest modulation scheme and error code) excluding error correction coding and the physical layer overhead. The typical throughput is what users have experienced most of the time when in useable range of the base station. Handsets also play an important part in throughput, and on some networks when close to the base station tests have shown data rates above the maximum specified rate, for example in tests using HSPA+ on an EE network a user got 25Mbps when HSPA is only rated to 22Mbps, so all figures should be taken as approximate. Latency times on mobile networks are also considerably higher than on terrestrial networks, 3G is typically 120 ms and 4G around 60ms

	Technology	Theoretical Max Down	Theoretical Max Up	Typical Down	Typical Up	Latency
2G	GPRS (Class 10)	85.6kbps	85.6kbps	20~35kbps	9.6Kbps	150ms
	EDGE Class 12)	236kbps	236kbps	50~144kbps	50~144Kbps	150ms
3G	EV-DO Rev. B	3.1Mbps	1.8Mbps	0.5~3Mbps	0.4~800Kbps	120ms
	UMTS HSDPA	14.4Mbps	0.384Mbps	0.38~7Mbps	0.38Kbps	120ms
	UMTS HSUPA	14.4Mbps	5.7Mbps	0.38~7Mbps	0.5~2Mbps	120ms
3.5G	HSPA+	42Mbps	22Mbps	9.24Mbps (EE)	12.4 Mbps(EE)	120ms
4G	4G / LTE FDD	150Mbps	50Mbps	20Mbp s(V.F)	10Mbps (V.F)	60ms
	4G/LTE Ad (MIMO)	3Gbps	1.5Gbps	150Mbps	75Mbps	60ms
5G	5G (MIMO)	10Gbps	Theoretical	Early trials achieved 2Gbps		

EE= Handset tested on EE. **V.F**= Handset tested on Vodafone

Note: that our table provides two download speeds: a theoretical maximum (based on the limits of the technology) and a typical download speed (which is more representative of what you'd actually experience).



The diagram above shows a typical mobile network, where a 4G/3G router is installed at the subscriber site and uses the mobile network to connect via the Internet to the In-Station

Potential problems with Mobile Networks.

With a mobile network a number of factors will affect its performance, not least is your distance from the local base station, other systems that may affect the mobile, and atmospherics. Network congestion can also be a problem, and if the network gets busy the first subscribers to be removed are those that connected first will be forced off the network, making them re-dial and establish a new call

Other issues that have occurred in the past have been major incidents, when everyone gets on their mobile phone, the network becomes saturated and emergency services were locked out of the network. There are now parts of some networks dedicated to the emergency services but this may not be available for traffic networks, so at a critical time when the network is most needed it may not be available.

Another issue with mobile networks is data integrity, as they tend to lose packets, which is not a problem when browsing the Internet or for voice calls but when running data it can be an issue. Running TCP helps with this, but it increases the network delays as the end systems have to re-transmit the data until it gets through.

Latency is also much greater on a mobile network than on a terrestrial network, typically 120ms on 3G and 60ms on 4G, without heavy traffic loads.

Another issue with a mobile network is providing security using IP Sec. This typically requires a fixed IP Address, and mobile networks don't usually provide fixed IP Addresses. There are companies which promise a fixed IP Address but they request you logon every night to re-fix your IP Address.

There are some routers which can solve this problem by using dynamic IP Addresses at one end to build a secure tunnel, (This is called FQDN (Fully Qualified Domain Name)). This relies on the host end Router having a fixed IP Address and a list of the pre-defined keys of users wanting to connect. A mobile network is very low cost to install but can run up significant bills in its operation.

Pros and Cons of using a mobile network	
Pros	**Cons**
Very quick to install	Have to control the costs or unexpected high bills
No cost of infrastructure	Need to be within range of base station
Reasonable data rate, varies depending on carrier, and location	Mobile networks not as reliable as terrestrial networks
	O.T.U Cabinet is usually metal, which blocks mobile signals – requires external (PuK) Antenna
	Security not as easy – due to difficulty of not being able to fix IP Addresses
	Possible to be 'bumped off the network' at busy times

3.3 CONSIDERATIONS WHEN OPERATING OVER A PUBLIC NETWORK

Backhaul – The data rate offered by ISP's is not the whole of the story. Once your data gets into the Telephone Exchange it uses a 'Backhaul' to take your data into the Internet. Most ISP's oversubscribe their backhaul, assuming that at any one time only so many users will want to connect to the internet. There will be times when the bandwidth being required is greater than the backhaul can support, in which case the traffic will be 'flow controlled' or packets dropped. Typically this could be at 3pm when children come home from school and power up their X-Boxes!!

The UK entrance to the Internet is in London at Tele-House or Rebus House in Docklands, so even though you're only sending data within your authority it will travel much farther.

Security – Because you're running over the Internet there is a risk of your data being hacked so security is extremely important?

Firewall - Your router should have a firewall which will block all incoming traffic unless you have told the router to accept traffic from that source or it allows traffic to pass through inside an IP Sec Tunnel.

VLAN – VLAN stands for a 'Virtual LAN' and this allows multiple devices to share a communications network but not to necessarily see each other's data. For example you may have a switch network and want to run your UTMC traffic on ports 3 and 4, CCTV on port 6 and maybe voice on port 8.

By using VLANS we can make ports the ports invisible to any users who are not members of that VLAN. VLANS can work over the entire network with the device (for example an ANPR Camera) attaching a tag to its data stream identifying it as a member of a specific VLAN, if the ANPR camera cannot add a VLAN Tag then switches can usually attach a VLAN tag to the data on the cameras behalf, making that device a member of a specific VLAN.

IP-Sec – Stands for IP Security and is the most important aspect of running sensitive data over the Internet. The routers at either end of the link form a secure encrypted tunnel between themselves and treat the internet as their own private network. This is one of the more complex things to configure and requires complete cooperation between network equipment suppliers. Some suppliers in traffic refuse to provide access to their equipment or provide the required configuration information, locking the authority into that network provider; this is completely unacceptable.

Reliability – In BT's words if you want a mission critical network then don't use the Internet. Most ISP's simply re-badge BT and there is a long standing problem within DSL broadband networks of the service hanging. If you're at home your ISP will tell you to re-boot your router but that's not so simple when the router is at the side of the road.

Some routers have a 'Health Check Monitor' built in which sends a message out to the internet at pre-defined intervals and if it gets a reply it knows the connection is healthy. However if it fails to get a reply it tries up to 3 different sites and then says 'the network has failed' and it restarts the line or restores service via 4G/3G etc.

3. PRIVATE NETWORK TECHNOLOGIES

3.1 LOCAL LOOP UNBUNDLING – PRIVATE BROADBAND NETWORK

The technology mentioned above as BT's SHDSL Network can also be built as a private network belonging to the authority. In this instance the network provider can work with BT Openreach to purchase the Copper circuits (Openreach call these Metallic Path facility (MPF)) at much lower costs than the authority purchasing the same circuits from BT Wholesale.

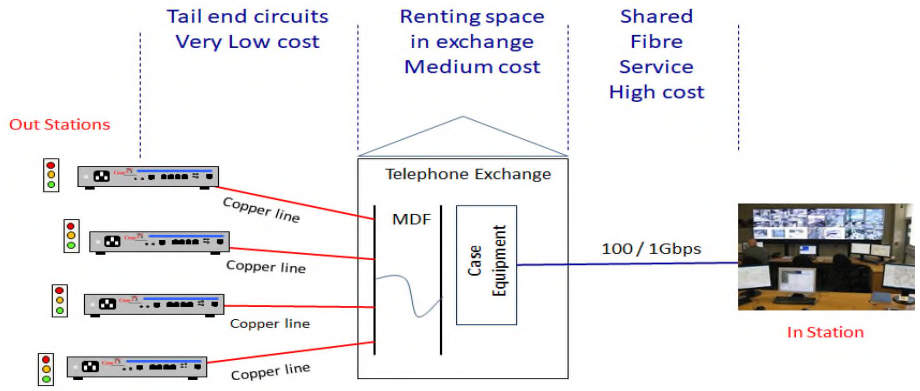
This involves the network provider installing equipment their DSLAM (Digital Subscribers Loop Apparatus Module) into the local telephone exchange, which provides a backhaul to the authority's central site.

The positive side of this solution is the authority will have a private Broadband Network, but the downside is the cost of installing equipment in the exchange and keeping it there can be quite high, and the cost of the backhaul to the authority can also be quite high.

To make this cost effective the authority will need a reasonable number of sites to connect to each telephone exchange. The exact number varies based on the location of the exchange and distance from the exchange to the authorities In-Station.

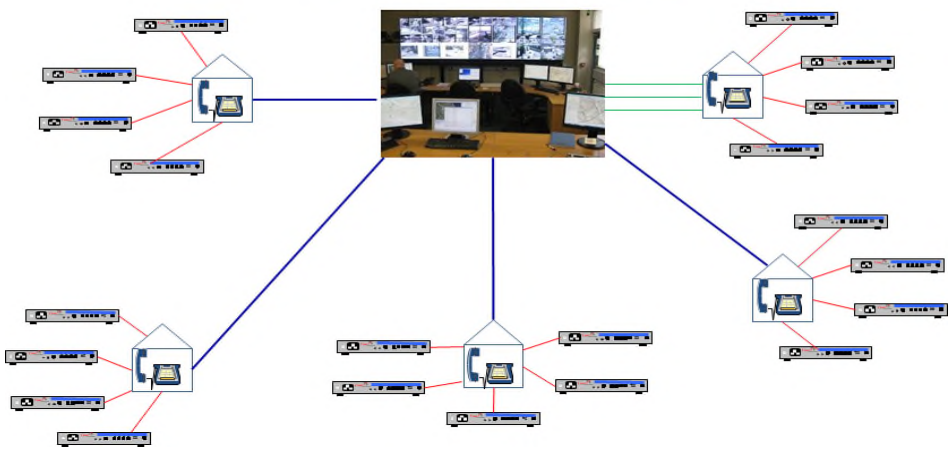
The positive aspects are that BT Openreach will provide an SLA on the copper circuits that BT Wholesale won't touch. The diagram below provides an overview of an LLU Solution

EFM (G.SHDSL) - LOCAL LOOP UNBUNDLING



While the diagram above shows a single exchange being used for Local Loop Unbundling in practice its likely that the Traffic Network will spread over several exchanges and will look similar to the network below.

EFM (G.SHDSL) - LLU NETWORK



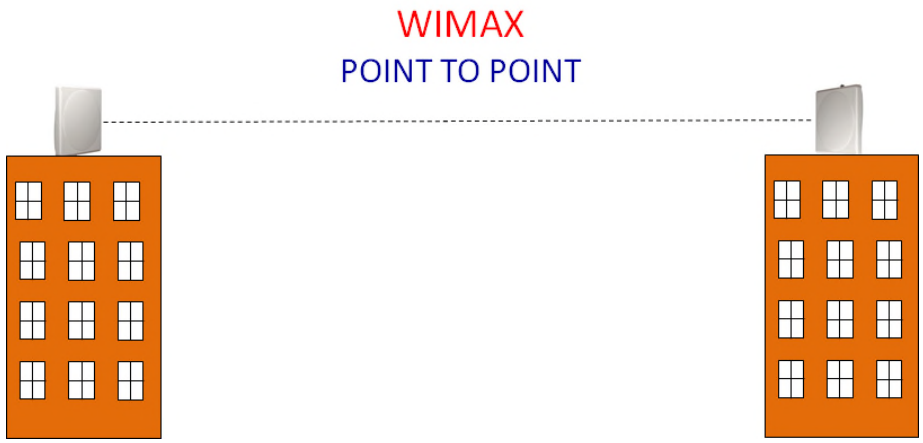
Pros and Cons of using a Local Loop Unbundling	
Pros	**Cons**
Private Network	Need enough sites to make it cost effective
Case EFM kit also fibre enabled easy upgrade path to Fibre	Customers not allowed in BT Exchange so need your network provider to install and support the network
BT Provide an SLA	
Copper circuits low cost	
Same bandwidth upstream as downstream	

3.2 WIMAX / WIRELESS NETWORKS

Wireless offers an excellent solution as it can be high speed, has low capital and low operating costs, but can also be a bit of a minefield. Over the past few years the 5Ghz frequency has been the most popular as it uses a 'Lite Licence', costing around £50 a year from Ofcom (if your provider bothers to get a licence). However, if someone installs a 5Ghz system close to your installation and it interferes with you , don't expect Ofcom to do anything about it

Point to Point Systems.

As the name 'Point to Point' describes, these wireless systems operate from Point A to Point B and have the greatest range, at theoretical distances to 60km, in practice typically more like than 10 - 15 miles, and ideally line of site (LoS) or Near Line of Site (NLOS).
5Ghz systems tend to use MIMO Technology (which stands for Multiple In / Multiple Out). In effect MIMO uses two radios inside one antenna, one working horizontally and the other vertically. The receiving end Antenna looks for these waves and catches as many of the signals as possible.
The diagram below depicts a WiMax point to point link



There are a wide variety of Wireless systems around some of the 5Ghz systems are incredibly cheap and they advertise data rates of 250Mbps, however these are the 'Over The Air' data rates not what you will receive at the Ethernet Interface. One customer asked us to look at their network and at 7Mbps, the wireless system's CPU was flat out at 99%, so maybe suitable for light data but not for video which is what they wanted it for.
Another consideration is whether the system is full or half duplex; many wireless systems work half-duplex so this may mean sending 700Mbps one way then waiting while the other end sends 700Mbps to you, although the time between send and receive is in milli-seconds. Generally this is not an issue as the bandwidth can be high enough to not be noticeable.
It's possible to tune some systems which for example may run at 700Mbps,to send a continual 600Mbps one way and 100Mbps the other, this is good for CCTV applications.

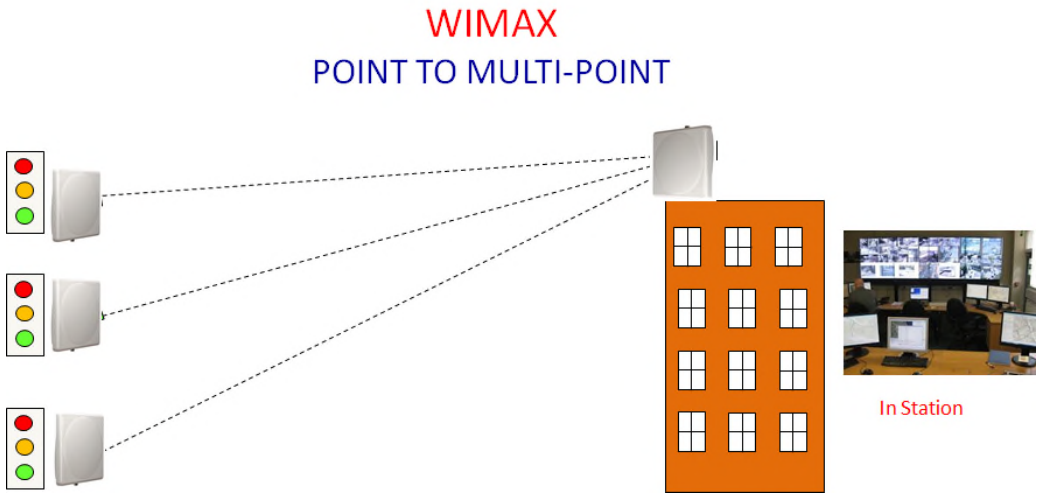
Gigabit 60Ghz to 80Ghz systems

There is another breed of Point to Point radios which use much higher frequencies (60Ghz to 80Ghz) to obtain higher data rates, typically 1Gbps or 2Gbps but for a limited distance of around 4 to 5 miles. These systems don't use MIMO but a fine pencil beam of radio and require much more rigid mounting and installation. The benefit of such a system is that there is much less chance of interference although you will still need a licence from Ofcom.

Point to Multi-Point

Wireless systems can also be point to multi-point. One station (generally called the 'Base Station') sends out a continual stream of data at 300Mbps, using a wide antenna of say 90degrees or even 120 degrees.

Several subscriber stations in this field will receive the data and will reply if the data is for them. This is a half-duplex system, so while all users can receive 300Mbps, sending data back the subscribers share the single 300Mbps so tend to be limited to say 50Mbps or 100Mbps. These systems operate over a shorter range.



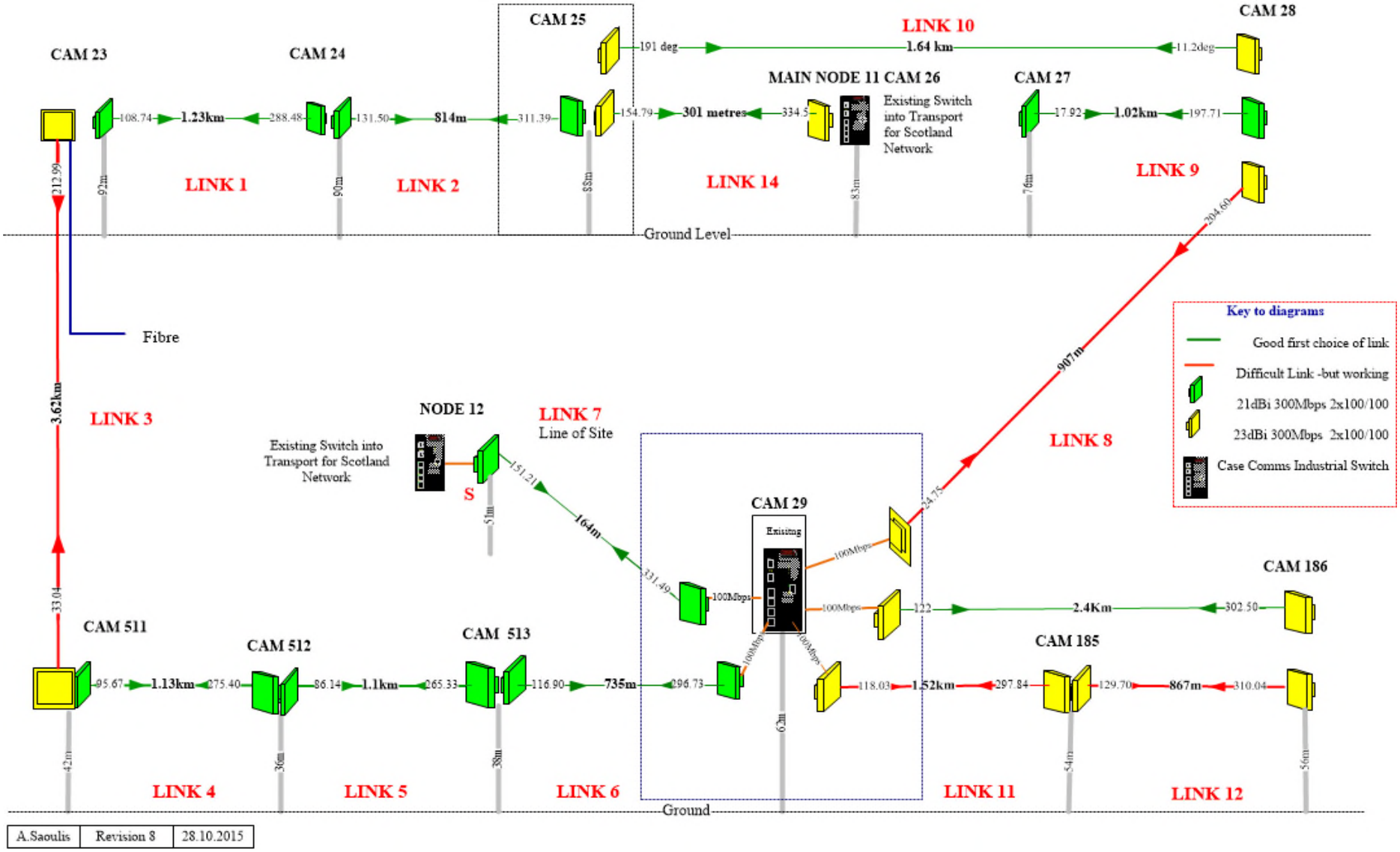
Why do some systems work and others don't?

Before considering the use of a Wireless system it's important to undertake a desktop survey and look at where the antenna are to be installed, and what obstructions (if any) are in the path. A link plot is taken to look at the terrain to make sure we don't have any major obstructions in the line of site.

Once the desktop survey has been undertaken the next stage is a full site survey. The site survey looks for interference in the area and also looks at what is required to undertake the installation, for example what metal work is needed to install the equipment, the length of the cable runs, where will the system be powered from and if cherry pickers are required or not. If you arrange a site survey make sure it's in the summer when all the leaves are on the trees, its great undertaking a survey in the winter and getting a very good data rate only to find when the leaves come out on the trees your data rate is reduced.

Pros and Cons of WiMax Networks	
Pros	**Cons**
Low Capex cost to install	Does not work everywhere – ideally L.O.S
Very low operating costs	2.4 / 5Ghz systems prone to interference
High Data Rates with quality system	Needs rigid installation for 60 ~80Ghz Systems
Secure and encryption is possible	
Private Network so secure	
Don't need to work with BT	

Diagram – A Case Communications customer wireless network –supporting CCTV



3.3 FIBRE OPTIC NETWORKS

Perhaps the ultimate is the authorities 'Own Fibre Optic Private Network'. Fibre has the highest levels of reliability, data integrity and performance and yet the lowest operating cost, but the capital costs of installing the fibre can be quite high. For authorities UTMC Networks 1 or 2Gbps is usually more than enough but even greater rates can be achieved, by bonding the Fibre trunks to achieve higher rates, typically 4 x 1Gbps trunks will achieve a 4Gbps pipe between switches. The next generation of Industrial switches already have trunk speeds of 10 Gbps.

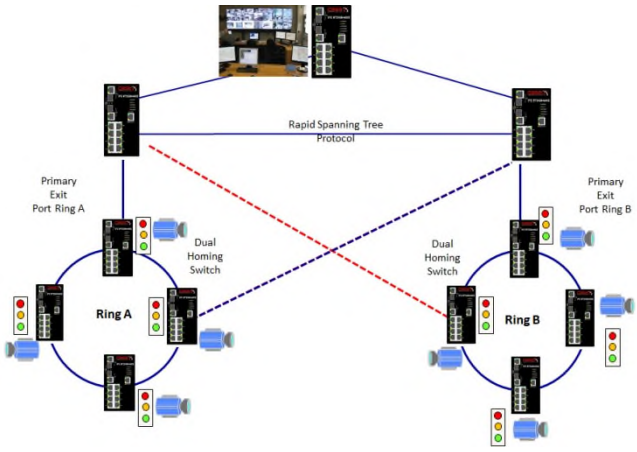
Industrial Ethernet switches use SFP's (Short form Pluggables) which are fibre optic drivers, driving distances over fibre up to 200km at Gigabit Rates.

Resilience

Most switches use the Rapid Spanning Tree Protocol (RSTP) which is re-routing protocol to self- heal the network in the event of a network failure within 6 to 10 seconds. But mission critical industrial switches designed for mission critical operation where the network cannot be allowed to fail for even 10 seconds and need more rapid self-healing, a technology known as 'Resilient-Ring' is used. Resilient Ring Technology allows, switches to self-heal in 10ms~20ms, and for this reason a network manager maybe unaware of a break in their fibre because the network has healed itself before anyone knows it has had a problem.

Dual Homing

As well as resilience within the ring it's possible to have dual exist points from the ring to the head end of the network. This is called 'Dual Homing' and can be seen in the diagram below. If either Ring loses its connection to the In-Station it can route via an alternate path



For this reason it's important to utilise a Network Management System, as described below

(VLANS) Virtual Local Area Networks.

With most modern networks it's possible to run multiple virtual applications on a common infrastructure and to divide these into virtual networks. These virtual networks spread across multiple switches in the network so for example UTCM could be on VLAN 1 and this means unless a device is a member of VLAN1 it cannot communicate with or see traffic on VLA1. We may have CCTV on VLAN 2, and perhaps Traffic Counters on VLAN 4.

Quality of Service

It's also possible to guarantee bandwidth for specific applications and also VLANS. For example we can allow CCTV to only consume 10Mbps per camera, UTMC to be guaranteed 10Mbps, and maybe public Wi-Fi 200Mbps. Using VLANS and QoS it's possible to share the network between multiple different traffic types, making it more cost effective.

Neale Burrows – Aberdeen City Council Senior Traffic Engineer

The Fibre Project itself was delivered as a 'Spend to Save', which including fibre costs etc. has less than a 5 year investment return.

As an estimate, it will have saved us £80-90k per year on Comms cost to traffic signals alone.

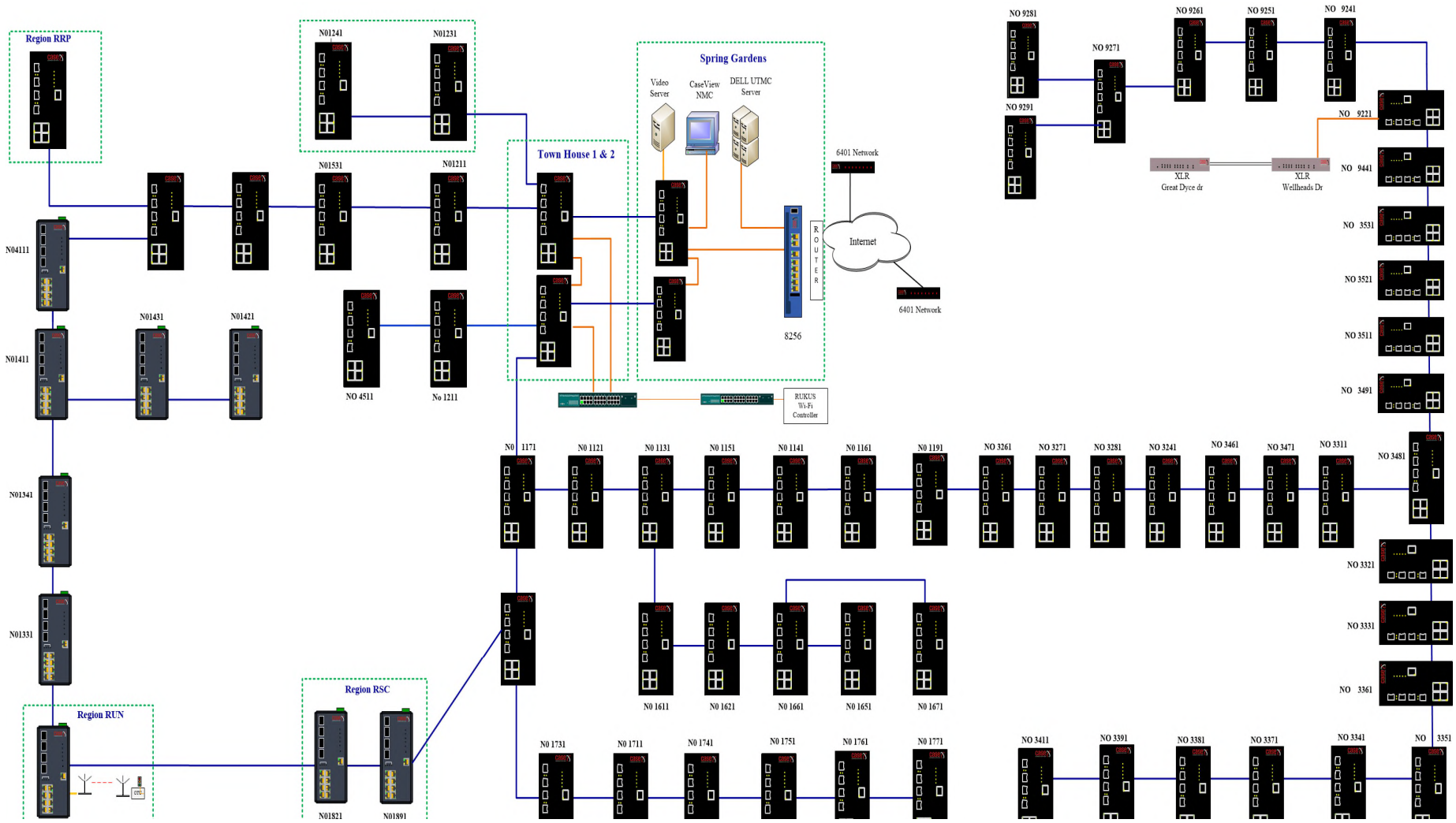
That said, additional benefits have been realised by having this infrastructure such as delivery of free city centre Wi-Fi, which was delivered at a fraction of the cost anticipated due to this infrastructure already being in place to support the deployment. We have also deployed out own CCTV network using the same connectivity and we believe that multiple use cases beyond traffic signals will be realised for multiple sensor deployments.

Neale Burrows
Engineer

Intelligent Transport Systems
Communities, Housing and Infrastructure
Aberdeen City Council
74 - 76 Spring Garden
Aberdeen
AB25 1GN

Email: nburrows@aberdeencity.gov.uk
Direct Dial: 01224 538049
Fax: 01224 538087

Aberdeen City Council Fibre Optic Network – supporting UTMC – CCTV – Traffic Counters – Public Wi-Fi



3.4 NETWORK MANAGEMENT SYSTEMS

It's important to use products that are managed using the SNMP (Simple Network Management Protocol). Typically the devices that manage networks are called Network Management Centres (NMC) or Network Management Systems (NMS).

An NMS supports many features which can be a great help to anyone running a network.

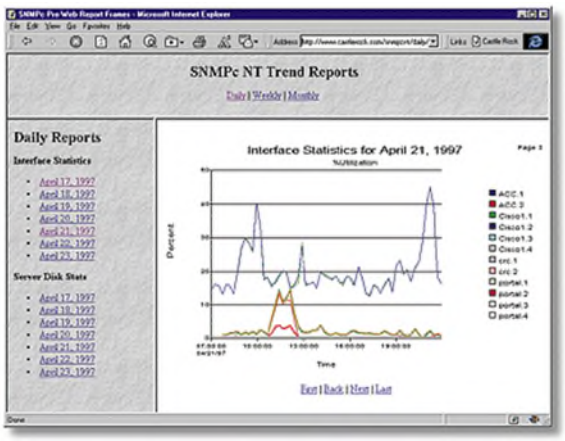
Monitoring the network status

An NMS sends a 'poll' to a network element (i.e. switch, router, even an O.T.U or logical IP Sec tunnel) and in the event the device fails to respond, logs a problem in the NMC database and changes the colour of the icon. The images below show a map of specific parts of a network. In the image to the left we can see most icons are Green, this means they are healthy and have nothing to report, an icon has turned blue- this means the unit has been re-started, one unit is yellow it has a problem which could become serious, and one icon is purple this indicates someone made a change – such as removed and replaced a cable.

In addition SNMP network elements (ie Routers, switches etc.) send messages to the NMS when they detect an event, for example someone unplugging a cable and putting it back. This is called an SNMP trap and it is logged in the database with a time stamp.

Trend Analysis

A network management is also useful to monitoring the status of your links, to see if they are noisy and about to fail or if the traffic loads are too great. The image below shows a typical trend report for a line between two routers.



Sending Alerts

A Network Management System should be able to send an e-mail or text message to the network manager in the event of a critical failure. This means that the on duty traffic engineer could receive a message while away from the In-Station and using remote access view the problem

Cost Versus Time

While an NMS is quite costly it has to be weighed against the time and stress of trying to diagnose network problems without such a tool.

A Network Management System should also allow a network manager to logon to the network and configure network elements or download configuration files, saving site visits.

APPENDIX A
Communication Network Acronym's

- **ADSL** – Asymmetric Digital Subscribers Line – ADSL2+ =24Mbps 'Annex M' 3Mbps Upstream
- **BGP4** – Peer to Peer routing used within the Internet
- **Bridge** – A device to join two local area networks together – operates at layer 2 – e.g. Switches
- **DSLAM** – Digital Subscribers Line Apparatus Module – In the exchange to connect your router.
- **EFM** – Ethernet First Mile – An Ethernet Extenders / Bridge which joins two local area networks and operates over Copper Circuits
- **Ethernet Switch** – A devices which connects multiple local devices on UTP / STP and allows them to go over a trunk to other switches.
- **3G Basic** – 1.5Mbps ~ 7.2Mbps
- **3G EDGE** – Enhanced Data Rates for GSM Evolution.
- **3G EVDO** – Evolution Data Optimised
- **3G HSDPA** – High Speed Download Packet Access
- **3G HSUPA** – High Speed Upload Packet Access
- **3G HSPA+ -** High Speed Packet Access Plus
- **FTTC** – Fibre to the cabinet. Uses V.DSL and what BT Call Fibre
- **FTTH** – Fibre to the home – fibre optic cable installed inside the premises
- **4G** – 15Mbps ~ 100Mbps
- **4G / LTE Advanced** – Advanced version of 4G downloads to 3Gbps
- **G.SHDSLbis** – One of the standards for EFM –G.SHDSLbis operates at 15.29Mbps per pair.
- **IEEE 802.16** – The formal IEEE Standard for WiMax
- **IEEE 802.11 a / b / c** –Standards for Wireless Networks.
- **IEEE 802.3** – IEEE Standard defining a LAN Physical, Data link, and Access should work. NB All products supporting Ethernet should conform to this.
- **IEEE802.3u** – IEEE Standard for Fast Ethernet 100Mbps
- **Layer 3** – In OSI (Open Systems Interconnection) L3 is a router allowing two different subnets to talk, as opposed to a layer 2 device which only allows devices on the same subnet to talk.
- **LLU** – Local Loop Unbundling –a network provider installed their equipment in the BT Exchange
- **LTE (4G)** – Long Term Evolution – mobile technology
- **MIMO** – A Wireless standard 'Multiple In, Multiple Out' using two antennas between radios
- **Multi-Mode** – Fibre optic cabling largely used within buildings with a maximum range of 2km
- **Mono (Single) Mode** – Fibre optic cable used externally for greater distance (up to 200km)
- **OSPF** – Open Shortest Path First – a more sophisticated routing algorithm used in larger networks.
- **RIP** – Routing Information Protocol – a method of data finding its way to its destination
- **Router** – A layer 3 (In OSI Terms) device which allows two different subnets to communicate.
- **TCP / IP** – Transmission Control Protocol – Provides error correction over an IP Network
- **SFP** – Short Form Pluggable – a Fibre optic driver in a plug in module.
- **SNMP** – Simple Network Management Protocol – a standard for managing network elements.
- **UDP** – User Datagram Protocol – A quicker way of sending data without error correction.
- **V.DSL** – Very high speed Digital Subscribers Line (Technology used with FTTC)

APPENDIX B

FACTORS TO CONSIDER WHEN SELECTING A NETWORK.

When deciding on the kind of network that a traffic engineer needs to implement there are a number of considerations to be taken into account, typically these could be

1. **Budgets** – both capital and operational, the bigger the capital budget generally the greater the savings that can be made and the lower the operational costs.

2. **Bandwidth**– These days there is an obsession with bandwidth, and customers look at the speed offered by ISP's. To be told that you can be offered a 25Mbps or 80Mbps Broadband data rate sounds great, but this is the very best rate into your local telephone exchange, what you don't know is what the backhaul data rate is. The backhaul is the circuit from the Telephone Exchange into the Internet and this is generally oversubscribed in the expectation that only so many customers will be using the backhaul at anyone time.

3. **Latency** – As well as bandwidth some applications can't tolerate delays in the network. If using the Internet this can never be guaranteed, as the Internet is an un-controlled network. Routers have a feature called quality of Service which says to the Internet, 'I am more important and need to go first', but as the internet is not controlled by anyone it can never work.

4. **Infrastructure** – what infrastructure is in place or possible? If you have ducts in place can you run fibre if not it can be very expensive to install ducts. Do you own your own copper?

5. **Physical Location** – some technologies are restricted by physical location. Typically WiMax systems can be affected by RADAR so working close to airports or ports can cause problems.

6. **Reliability** – While everyone wants a reliable network, at times it's tempting to purchase non industrial equipment, which is typically used in an office environment. These products may work well for a period of time but its important to way up the cost of having to visit a site two or three times a year against spending more on a product and not having to visit.

7. **Management and control** – with a large network one of the most important aspects is the ability of the traffic engineer to have control of the network. Products that support the management protocol called SNMP (Simple Network Management Protocol) can save the network manager a lot of time and trouble in diagnosing problems and planning their network, as well a providing an SLA.

8. **Who owns the network?** – In I.T. networks its vital vendors work with each other to gain an understanding of the equipment in the network path and to provide a solution for their customers. Any vendors that deny their customers access to their own equipment, hold their customers to ransom.

APPENDIX C

TECHNOLOGIES DATA RATES, LATENCY, AND RELIABILITY						
Technology	**Lay**	**Max Data Rate In Theory**	**Typical Latency**	**Real-Time Video**	**Data Integrity**	**Reliability**
ADSL	3	Max 24 / 3Mbps	Av30~40 ms	Not good	Good	Average – ISP Dependant
V.DSL	3	Max 80 / 20Mbps	Av30~40 ms	Good	Good	Average – ISP Dependant
G.SHDSL / EFM	2	Max 60 / 60Mbps	Good	Good	Good	Good–depends on copper
Mobile 3G EVDO Rev B	3	4.9 Mbps / 1.8Mbps	Typically 120ms	Poor	Can Suffer Packet Loss	Medium-Dependant on network
Mobile 3G HSDPA	3	14.4Mbps / 0.38Mbps	Typically 120ms	Acceptable	Can Suffer Packet Loss	Medium-Dependant on network
Mobile 3G HSUPA +	3	14.4Mbps / 5.7Mbps	Typically 120ms	Acceptable	Can Suffer Packet Loss	Medium-Dependant on network
Mobile 3G DC-HSPA+	3	42Mbps / 22Mbps	Typically 120ms	Good	Can Suffer Packet Loss	Medium-Dependant on network
Mobile 4G / LTE	3	100Mbps / 75Mbps	Typically 60ms	Good	Can Suffer Packet Loss	Medium-Dependant on network
Mobile 4G / LTE Advanc	3	3Gbps / 1.5Gbps	Typically 60ms	Good	Can Suffer Packet Loss	Medium-Dependant on network
WiMax 5Ghz Typical	2	100 ~ 300Mbps	Good	Very Good	Possible Interference	With good design – 99.999%
WiMax – 60~80Ghz	2	1 ~ 2Gbps	Good	Very Very Good	Good	With good design – 99.999%
Fibre	2	1 ~ 10Gbps	Very Good	Very Very Good	Very Good	Very good

NB. Lay = The network layer these technologies operate at. To allow two different subnetworks to talk requires Layer 3.

APPENDIX D

Communications Protocol Stack

TCP / IP Architecture Versus the OSI Model

The network Hardware is largely concerned with the Physical Layer (i.e. Fibre, Copper, and Wireless) to the Transport Layer TCP or UDP.