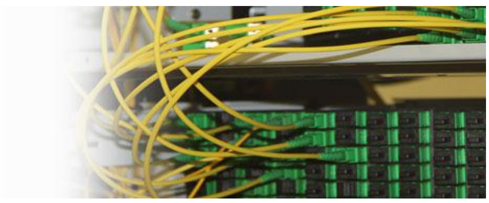
Broadband Communications Options for Public Safety Agencies

December 2012

THE UNIVERSITY OF MELBOURNE

Australian Broadband Applications Laboratory
Institute for a Broadband-Enabled Society



Scope

The focus of this report is on broadband requirements for current and future applications for use by Public Safety Agencies (PSAs) in day-to-day activities as well as extreme events that may impact on large numbers of people. The report considers delivery options for PSAs that would complement a dedicated mobile wireless network.

Information in this report has been compiled on the basis of desktop searches, as well as in house knowledge of the Australian Broadband Applications Laboratory at the Institute for a Broadband-Enabled Society, the University of Melbourne.

Biographies of authors

Kate Cornick has a PhD in optical communications. She has worked as a Senior Advisor and Deputy Chief of Staff to Senator Conroy, Minister for Broadband, Communications and the Digital Economy. She is currently the Executive Director of both the Australian Broadband Applications Laboratory and the Institute for a Broadband-Enabled Society, where she drives research and development in broadband applications and innovations. Kate has authored a number of white papers on digital strategies and the future broadband-enabled society.

Brad Gathercole has been designing and deploying mobile phone networks in the Australian telecommunications industry for over a decade and is currently the Chief Technology Officer of the Australian Broadband Applications Laboratory (ABAL), co-located with the Institute for a Broadband-Enabled Society (IBES). Brad has worked on the site design and deployment of the Optus' GSM and 3G networks and as a Senior Transmission Engineer at Kordia Australia, where he was responsible for the transport design of the Vodafone 3G network in Melbourne and Adelaide. Prior to joining IBES, Brad was at Telstra focusing on the design and specification of the Ethernet backhaul network to support Telstra Next G mobile base stations.

Contents

Executive Summary

Public Safety Agencies (PSA) broadband communications needs are growing. To meet the demand for services PSAs have been allocated 5+5 MHz spectrum by the Australian Government, which they can use to establish a dedicated mobile wireless communications network across the country. The network is expected to make use of Long Term Evolution (LTE) technology, and should meet PSA communications needs under business-as-usual conditions.

In some circumstances, where the number of deployed PSA personnel who require access to communications technologies is high, a dedicated LTE network may not meet PSA broadband demands, no matter how much spectrum is made available. This includes incidents at major venues, involving large numbers of general public, as well as incidents at random locations that are rare and unpredictable such as natural disasters. In addition, the PSA network will not cover the entire Australian continent and further, network redundancy options may be required in some circumstances, for example in the event that part of the PSA network equipment is damaged through fire.

To meet PSA broadband demands under these circumstances different broadband communications options are required to complement coverage provided by the PSA mobile wireless communications network, and importantly to add capacity, redundancy and reliability to PSA services. Different broadband communications options may also assist with reducing the cost of the rollout of a dedicated PSA mobile wireless network.

This paper considers different options for PSA communications that would complement a PSA mobile wireless network, including roaming onto commercial LTE networks, satellite communications and the use of Cells on Wheels (CoWs) and WiFi technologies, all of which can add redundancy and increase the availability of broadband capacity to PSA personnel.

The paper also discusses the role of the National Broadband Network, which provides a unique solution for the Australian environment that is unavailable to many other countries, and could position the country as a global leader in PSA communications providing enhanced and future-proofed capacity as well as network redundancy and resilience, when used in conjunction with a dedicated PSA LTE network. This includes through the use of the 'Fourth Port' on NBN connected buildings, as well as 'Data Hydrants' that could be made available in easily accessible locations for PSA personnel.

Combining different broadband access options with different local backhaul solutions, such as the NBN, provides PSA with a diverse range of options to meet current and future communications needs during incidents at major venues and at random locations. It is highly recommended that PSAs explore these options further to ensure any dedicated PSA wireless communications network can be used in conjunction with other access technologies to add redundancy, capacity and reliability to PSA communications services.

1 Introduction

Demands for broadband communications access by Public Safety Agencies (PSAs) are growing, as new broadband applications come to market that could improve decision-making and incident responses.

To cater for increasing broadband usage, PSAs have been pursuing the establishment of a dedicated wireless communications network that uses state-of-the-art Long Term Evolution (LTE) technology. The Government has recently assisted with this, by announcing that 10 MHz of spectrum in the 800 MHz band will be made available to PSAs to meet their communications needs[1].

The vast majority of PSA communications needs are 'business-as-usual', and may involve responding to incidents that involve a number of people. Business-as-usual activities assume that only a limited number of response teams are required, meaning a limited number of PSA personnel are involved in communications, including between incident control centres and the incident site. A dedicated PSA LTE wireless network is expected to cater for these needs in most circumstances[2].

Some incidents may require a much larger PSA response compared to business-as-usual activities, including for example natural disasters, terrorist attacks or incidents where a large number of people may be involved. Having broadband network capabilities to support a high demand for PSA communications could be critical to the success of a response. These sorts of incidents can be broadly split into two categories:

- **Incidents at Major Venues (IMVs)** include large-scale incidents that occur at venues where a large number of people regularly congregate, for example venues where sporting events and music festivals are held regularly, as well as metro train stations and major shopping centres. The area affected by an incident at a major venue is likely to be small, in the order of a couple of square kilometers (km^2). Because the number of people at risk from any IMV is high and the number of locations where such incidents may occur is limited, PSAs should ensure additional communications infrastructure is in place (over and above a dedicated PSA LTE network) prior to any incident occurring. The infrastructure may be permanent (for example, in the case of major train stations or shopping centres), or may be temporary (for example, in the case of an annual sporting event such as the Spring Racing Carnival in Melbourne).

- **Incidents at Random Locations (IRLs)** are large-scale incidents that are rare and unpredictable in terms of where and when they may occur, and they infrequently occur in the same location. The area affected by an incident at a random location is likely to be large, ranging from 10 km^2 to greater than 100 km^2. Given the size of Australia's landmass it is highly unlikely that a dedicated PSA LTE network would be available for many of these incidents. They will need to quickly establish capabilities that support high demands for broadband communications. Examples of IRLs include natural disasters such as bushfires, cyclones or floods.

This report considers the additional communications needs of PSAs over and above a dedicated PSA LTE network, in particular for incidents at major venues and random locations. This is for three reasons: firstly, a dedicated PSA LTE network will not cover all the Australian landmass and mobile roaming and satellite services will need to be used in regional areas. Secondly, redundancy options are needed given the high risk that during major emergencies, mobile phone towers may be rendered unusable, for example during power outages caused by fire or flooding, resulting in communications blackspots. Finally at incidents where a high concentration of PSA personnel are expected to be using communications, the volume of data may be such that no terrestrial mobile broadband network could cope.

This report explores the categories of communications technologies that may be required by PSAs into the future in Section 2. Section 3 provides an introduction to broadband technologies and Section 4 further explores these technologies for use by PSAs. A conclusion is provided in Section 5.

2 Overview of Apps

Modern day fixed, wireless and satellite broadband networks have the capability of simultaneously delivering voice, video and data services to end-users. These different types of service offerings are commonly referred to as triple play services and are a key capability of next generation broadband networks. Both public and private entities, including governments and their agencies, are increasingly making use of services and applications enabled by these networks to drive innovation, productivity and improve customer interfaces.

As broadband network access becomes ubiquitous across Australia, the PSAs will increasingly take advantage of broadband networks to better respond to a range of incidents, including business-as-usual events, incidents at major venues and incidents at random locations.

This section outlines the sorts of technologies that will underpin applications that PSAs may use into the future in all three classes of incidents.

2.1 Voice communications

Voice communications are an integral part of any coordinated response to an incident. Due to the inherently mobile nature of PSA response personnel, mobile voice communications are imperative for business-as-usual, and incidents at major venues and random locations.

Voice bandwidth requirements are minimal, requiring speeds of around 21 kilobits per second (kbps) to 87 kbps depending on the codec used to encode the voice transmission[3]. However, while bandwidth demands are small voice communications quickly becomes unintelligible if delays in transmission are experienced. For this reason, voice is typically prioritised over data and video traffic on broadband networks.

2.2 Push to Talk

Push-to-Talk on mobile networks is a feature that emulates the behaviour of a traditional walkie-talkie enabling only one user on the network to talk at any one time. Push-to-Talk is a half duplex transmission where one user “pushes” the button on their terminal to talk, while all other users are able to hear the transmission.

Push-to-Talk applications are currently used by PSAs over radio networks, enabling incident control centres to coordinate many different personnel in the field without having to directly call each of them. The benefit of deploying push to talk over mobile broadband is that the potential coverage area is much larger than may be achieved with a dedicated two-way radio network when taking into account the existing coverage offered by the commercial carriers.

Like voice communications, Push-to-Talk applications requires mobility. The application has low bandwidth requirements requiring speeds of about 28 kbps, but is highly susceptible to delay.

2.3 Messaging services

Messaging services similar to a traditional mobile network SMS can be used by PSA personnel to quickly provide other PSA personnel with information when a voice service is not required. This could be the case for business-as-usual, and incidents at major venues and random locations.

The disadvantage of messaging services is that, like SMS messages, the delivery is not necessarily guaranteed to be instantaneous. Messaging services typically require very low bandwidth.

2.4 Video conferencing

Video conferencing consists of two-way communications combining both video and audio data streams. The use of videoconferencing is becoming increasingly common in business and personal communications, largely due to the increased availability of high-speed broadband and increasing interoperability between video conferencing platforms.

There are currently two types of solutions for video conferencing:

- ***Dedicated telepresence systems*** require dedicated hardware to be installed at both end-user locations and typically make use of managed broadband services that ensure a very high quality experience. Dedicated telepresence systems have the advantage of offering a high-end, secure and rich immersive experience. The video stream is typically high definition, and as a result the required bandwidth is typically large. However, the experience is 'life-like' meaning very small details can be perceived from the video conferencing footage.
- ***Cloud based teleconferencing solutions*** do not require dedicated hardware and can be installed on different devices. Examples include Skype, Cisco's WebEx platform and Vidyo [4][5][6]. Cloud based teleconferencing solutions are cheaper to deploy compared to dedicated telepresence systems, however the quality of the video can depend on the availability of network capacity and in some cases finer details cannot be perceived from the video conferencing footage. As a result cloud based teleconferencing solutions are currently prone to pixilation and audio dropout, however this is expected to become less of a problem as high-speed broadband services become more widely available. Cloud based video-conferencing services are also increasingly able to dynamically adapt the video quality of the call based the available network capacity. Some cloud-based solutions, in particular free services, have limited security features although they are increasingly making use of encryption[7].

Figure 1: Dedicated Telepresence System

Video-conferencing is likely to be increasingly used by PSAs into the future for a range of incident responses including business-as-usual activities, as well as in incidents at major venues and random locations. Uses of video conferencing by PSAs include communications between incident control centres, experts and PSA personnel in the field, for example a doctor could communicate to an ambulance paramedic regarding the first aid treatment of a patient[8].

The speed and bandwidth requirements for video conferencing applications vary. Full high definition videoconferencing, such as that supported by dedicated telepresence systems, requires broadband speeds of at least 4 Megabits per second (Mbps) in each direction. Cloud based teleconferencing solutions can also cater for high definition video, so long as high capacity broadband is available, but also supports standard definition video that may require speeds as little as 128 kbps in both directions[9].

PSA broadband requirements to support video conferencing will vary. For incidents at major venues and random locations where a large number of PSA personnel may be present, many video connections may be required and as a result broadband requirements can be large.

2.5 Video Streaming

Video streaming consists of a one-way video transmission, potentially combined with an audio stream.

Examples of uses of video streaming by PSAs include footage from permanent or temporary surveillance cameras or helmet mounted cameras worn by PSA field personnel, that is sent via a broadband network to a central incident control centre to assist with decision making. Video may also be streamed to PSA personnel in the field to aid with responses.

As per the videoconferencing requirements, a high definition video stream will require broadband speeds up to 4 Mbps while a standard definition video needs as little as 128 kbps. Video streams could be accessed either in real time or at a later date using store and forward capabilities. These different video streams have different requirements:

- Real time video streams need to be transmitted without delay, therefore the broadband network must have the capacity to support the data rate.
- Store and forward video streams, for example from a surveillance camera, could be transmitted when network capacity is available.

2.6 Images

Images can be downloaded or uploaded to and from personnel in the field for a number of reasons including supporting decision-making across the full range of PSA activities. Examples of images that may need to be accessed by PSAs include building plans to help direct PSA personnel or photographs of criminals to assist with identification at an incident.

Image sizes can vary considerably, requiring broadband speeds ranging from kbps to Gigabits per second (Gbps) in order to support timely transmission. As a result, the time to transfer images depends on the size of the image file and the available network capacity. The transfer of large image files may be limited by long transmission times if sufficient network capacity is not available. However, in some cases store and forward transmission may be used when sufficient capacity becomes available.

Traffic from image transfers may also vary significantly between responses. At incidents at major venues and random locations, where large numbers of PSA personnel may be present and require information such as building plans, a lot of images may need to be transferred and this could consume considerable bandwidth.

2.7 Database access and cloud computing

Database access and cloud computing applications are key capabilities that are increasingly used with the deployment of high-speed broadband networks. PSAs are likely to make increasing use of remote database access and cloud computing technologies to assist in responses to incidents. Examples include accessing PSA databases, for example police databases to identify criminals, or medical records to aid the first aid treatment provided to a patient at an accident.

The bandwidth requirement of cloud computing depends on the type of data being accessed, and as a result speed requirements are expected to vary from kbps to Gbps, and may also include image downloads. As with image transfers, remote database access may be limited by network capacity.

2.8 Sensing and Monitoring Devices

Sensing and monitoring devices such as motion detectors and smoke and fire alarms can provide valuable information to PSA personnel attending an incident. These types of devices send small amounts of data back to a monitoring station, which could be accessed by PSA personnel to aid decision-making.

As the data involved in this type of communications is typically small, the broadband speed requirements would be in the order of kbps assuming no video is used.

2.9 Augmented Reality Environments

While augmented reality applications are in early stages of development for commercial use it is expected that they will play an increasingly important role for PSA personnel over the next 5-10 years [10]. For example, augmented reality applications could be used in central incident control centres and in the field to provide additional information in a more user-friendly format. These applications will give an improved understanding of a localised area and will assist with decision-making and incident responses. Examples of augmented reality applications include an immersive 3D environment of a building, or live video streams of real world environments with computer generated information overlayed on top.

Depending on the application, augmented reality environments could require broadband speeds ranging from kbps through to high definition 3D video streams that can require in excess of 8 Mbps. Therefore the transmission of augmented reality applications will be impacted by network capacity.

2.10 Remote Controlled Devices

Remote controlled devices such as robots can be used to enter an environment and perform an operation where it is too dangerous for PSA personnel. These types of devices could be enabled to provide both video and audio feeds as well as control of the robotic tools to interact with the environment.

Assuming standard definition video streams are used, the broadband speeds required to operate remote controlled devices are likely to be in the range of tens of kbps to Mbps.

2.11 Summary

In the future PSAs are likely to make use of an increasing number of broadband applications to support their decision-making and responses to business-as-usual, and incidents at major events and random locations. The increased use of broadband applications by PSAs will require dedicated telecommunications resources to support the transmission of the voice, data and video traffic. The next section outlines the components of the telecommunications infrastructure that facilitate general communications across Australia.

3 Broadband Overview

The Australian national telecommunications infrastructure consists of a number of ad-hoc interconnected networks that can be broadly split into different components including backhaul, fixed access, local wireless access, mobile wireless access and satellite networks. This section describes the functionality of these networks.

3.1 Fixed Access Networks

Fixed access networks rely on a physical cable connection between an end-user premises and a telecommunications exchange. There are four access technologies that are commonly used today:

- ***Digital Subscriber Line (DSL)*** technologies make use of traditional telephone networks' copper twisted pairs. Theoretical speeds vary according to DSL technology, distance between the end-user premises and the exchange, as well as the quality of the copper. Theoretically, ADSL technologies provide 8 Mbps downlink and 1 Mbps uplink over distances of up to 1.5 km; ADSL2+ provides 24 Mbps downlink and 1.1 Mbps uplink over distance of up to 1.5km; and VDSL2 provides up to 100 Mbps downlink and 30 Mbps uplink over distances of 800m[11,12].

- ***Fibre-to-the-Node (FTTN)*** makes use of optical fibres and DSL technologies to improve achievable broadband speeds. This is done by reducing transmission distance between end-user premises and active DSL components, which are installed in 'nodes' closer to homes rather than in telephone exchanges. Optical fibre transmission is used to connect the nodes back to the telephone exchange.

- ***Hybrid Fibre-Coax (HFC)*** cable technology is currently deployed in some metropolitan areas across Australia and is used to provide cable TV and internet services. HFC Cable networks are able to support much larger data rates than copper twisted pair with theoretical maximum rates of 100 Mbps in the downlink and 10 Mbps in the uplink direction, however broadband speeds are shared between users on the network so actually speeds are likely to be a lot slower[13].

- ***Fibre-to-the-Premises (FTTP)*** technologies make use of optical fibres that connect end-users to telephone exchanges. FTTP technologies provide improved broadband speeds over HFC or DSL technologies. FTTP broadband speeds are not limited by distance in the access network, so synchronous speeds in excess of 10 Gbps are achievable[14]. Today, the National Broadband Network is being rolled out in Australia and is offering speeds of 100 Mbps downlink and 40 Mbps uplink, using Gigabit Passive Optical Network (GPON) technology (see Section 3.6 for more information)[15].

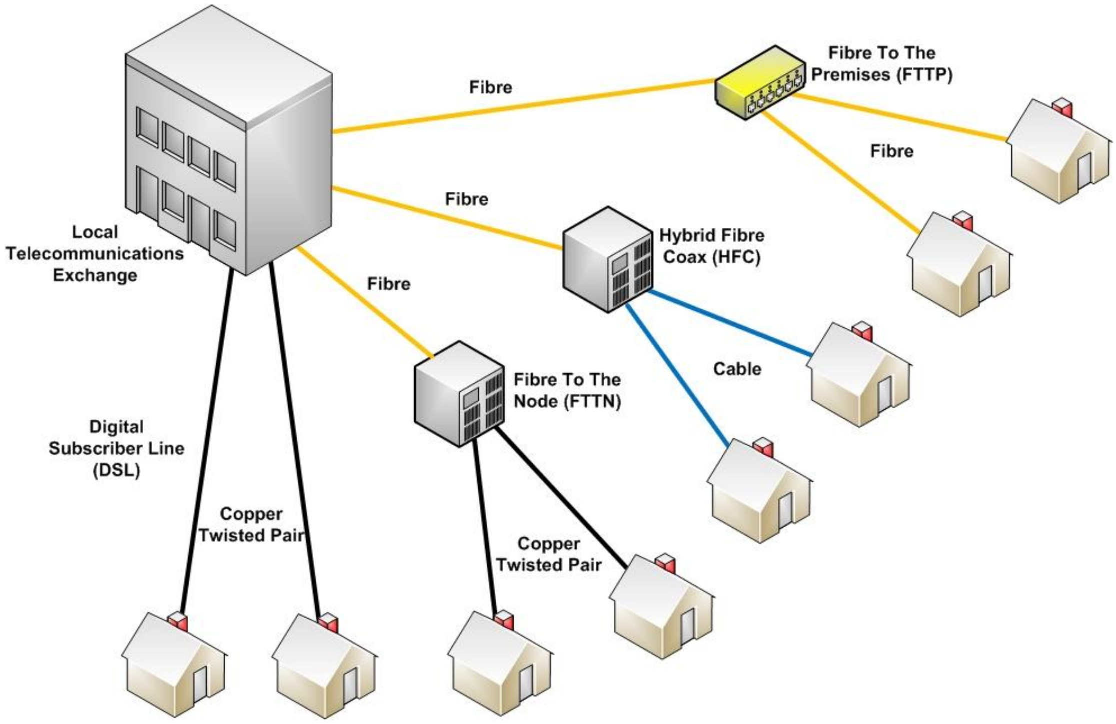


Figure 2: Fixed broadband access technologies

Fixed telecommunications networks are the most reliable broadband service, as environmental conditions do not tend to impact on transmissions, especially if cables are buried underground. Fixed services are also secure: interception is difficult to achieve and the high bandwidth means that the highest levels of encryption may be used without impacting the level of service. Fixed networks are also able to be configured to provide quality of service.

3.2 Mobile Wireless Broadband Access

Mobile wireless broadband access relies on radio communications in the 800 MHz – 2 GHz range between base station sites and mobile-enabled end-user devices[1]. The base stations are connected via backhaul networks.

Base stations can provide coverage over distances ranging from a few hundred metres up to 200km depending on the spectrum used[16]. However, mobile broadband speeds are impacted by a number of factors including base station configuration, signal strength and interference from neighbouring base stations. Mobile wireless is also impacted by end-users constraints including their location (dense vegetation or topographical features may impact on coverage), the number of simultaneous users in the local area that share the capacity of a base station and the quality of end-user equipment[17] . It is also difficult to guarantee a certain level of service as users roam from one base station to another while maintaining a constant connection.

In Australia the most common mobile wireless broadband technology is based on the 3GPP UMTS network standard. Theoretical speeds on these so called 3G networks are quoted as 42 Mbps downlink and 11 Mbps uplink and are for a

[1] This is an approximate guide and 700 MHz spectrum may become available subject to the digital dividend auction.

single user in ideal conditions hence are unlikely to be experienced in a real world scenario [18]. The latest mobile wireless broadband platform being rolled out in Australia is based on the 3GPP Long Term Evolution (LTE) standard. LTE networks are currently capable of theoretical speeds of 300 Mbps in the downlink and 170 Mbps in uplink with projected theoretical downlink speeds in the order of 1 Gbps downlink and 500 Mbps uplink in the future [19]. To achieve these speeds large allocations of spectrum are required, and only a single user can access the base station at any one time. LTE networks also share the same limitations as current 3G networks so the quoted theoretical speeds are unlikely to ever be experienced by an actual user.

Mobile wireless networks security is dependent on the level of encryption used between the end-user device and the base station. Commercial network providers have these security features enabled by default.

3.2.1 Commercial Mobile Wireless Broadband Operators

There are three commercial providers of mobile wireless broadband services in Australia: Telstra, Optus and Vodafone. Telstra currently has the largest network, covering 99% of the Australian population[20]. Optus and Vodafone coverage currently extends to 97% and 94% of the population, respectively[21,22]. However, while the population coverage is high, the actually percentage of the Australian landmass covered by commercial wireless broadband operators is low. Telstra is the only provider that publicly states its landmass coverage at 2.1 million square kilometers, corresponding to about 27.3 % of Australia[23]. Much of the coverage in rural areas requires the use of high quality handsets with external antennas to extend coverage.

Telstra and Optus have both launched LTE networks in the capital cities, with Vodafone announcing they will launch their LTE service in early 2013[24]. All three networks offer 3G services, with Telstra quoting LTE speeds of up to 40 Mbps in some locations[25].

3.3 Local Wireless Broadband Access

Local wireless broadband networks include WiFi technologies which make use of fixed, or in some cases mobile wireless, access networks. A WiFi router provides high capacity wireless communications access over small distances of up to 450 m[26]. WiFi technologies make use of radio spectrum in the 2.4 GHz and 5 GHz bands for public use and 4.9 GHz band for public safety use[27,28]. The benefit of WiFi communications is that it extends the coverage of the access network, and in the case of fixed access technologies provides otherwise unattainable mobility in a local area.

Local wireless broadband networks are commonly used in the home to enable mobility while making use of fixed broadband connections, or by organisations to provide broadband access for mobile devices such as smartphones and laptops in specific geographical areas (e.g WiFi hotspots). Local wireless networks are also used by commercial mobile wireless network operators to free up capacity on their networks by providing an alternative way to connect to the internet in areas where demand for services are high, e.g. in shopping centres.

The speeds that can be achieved on local wireless networks are highly dependent on the type of access technology used for connectivity, the number of users or devices using the network and the number of wireless access points available for people to connect to. The latest WiFi standard (802.11n) supports theoretical downlink speeds up to 300 Mbps, though this requires the end-user terminals to be capable combining two wireless signal together, known as channel bonding. If WiFi terminals are not capable of channel bonding, then the available bandwidth enables broadband speeds of approximately 150 Mbps[29].

Public local wireless access generally provides a lower level of security compared to fixed and mobile wireless networks, however this is highly dependent on the encryption techniques used between the end-user device and the WiFi router. The coverage area for local wireless networks is small, and as a result is generally not affected by environmental conditions. As a result the reliability of the service is generally consistent. Local wireless access for PSAs provide an alternative communication platform that can be accessed to offload data and free up resources on the dedicated LTE network or to provide a redundant communications path in the event of an outage on the LTE network.

3.4 Satellite Broadband Access

Satellite services use two radio links typically in the 1 GHz to 18 GHz range: one to connect a user to a satellite station in space, and the second to the satellite station in space to a ground station[30]. The ground station is typically connected to a fibre backhaul network. Users accessing satellite services require a dedicated user terminal or satellite dish. Satellite broadband services have limited capabilities compared to terrestrial broadband solutions, and are typically used for communications in remote locations that are not serviced by terrestrial broadband network.

Due to the transmission times between the user terminal and satellite and the satellite and ground station, latency can have a negative impact on time sensitive applications. Satellite communications are also particularly susceptible to atmospheric conditions such as heavy rain, humidity and bushfire smoke with the performance degrading when these conditions are present[31].

Today, satellite broadband speeds typically are in the order of 6 Mbps in the downlink and 1 Mbps in the uplink[32]. Future satellite speeds will be in the order of 12 Mbps in the downlink and 1 Mbps in the uplink[33]. These next generation satellite services will provide significantly improved speeds and capabilities and will significantly improve issues such as latency and support for time sensitive applications.

Like other forms of wireless communications the level of security over satellite broadband is dependent on the encryption technologies used. However, it is noted that high levels of encryption technologies require significant overheads and this may affect satellite broadband performance as overall capacity is limited compared to terrestrial solutions.

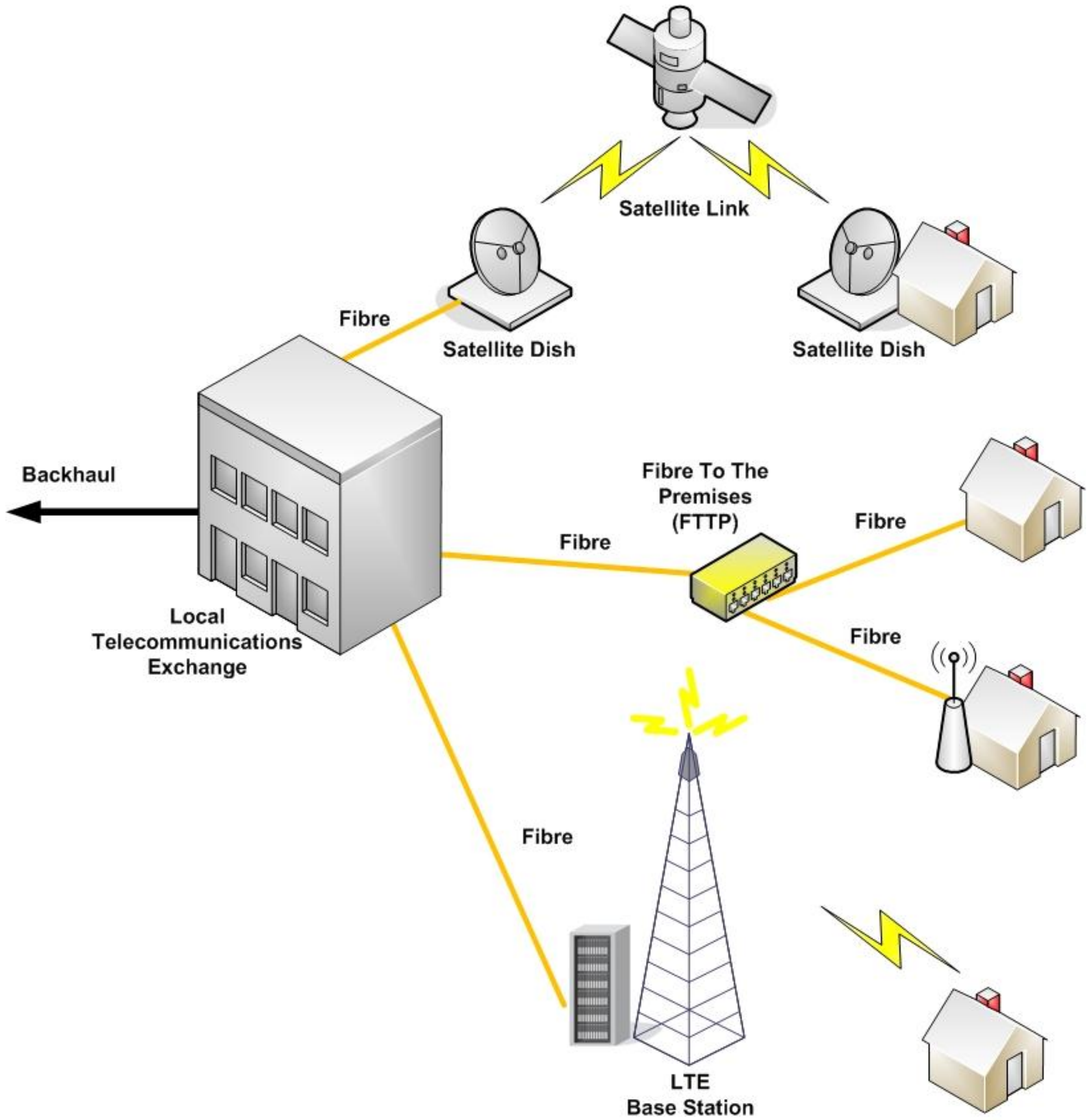


Figure 3: Telecommunications access networks

3.5 Backhaul networks

Backhaul networks provide interconnectivity between telephone exchanges (in the case of fixed networks), base stations (in the case of mobile wireless) and ground stations (in the case of satellite networks). Backhaul networks traverse many hundreds of kilometres between suburbs, cities and states and are designed to transport huge volumes of data.

The most efficient and reliable backhaul technology makes use of fibre optic cable, which is capable of transmitting terabits of information along a single fibre. As backhaul cables are typically buried, optic fibre backhaul networks are not generally impacted by topographic or atmospheric conditions, making them inherently stable.

In some cases microwave radio is used to provide backhaul services, particularly to connect remote wireless base stations back into the fibre backhaul network. Microwave radio makes use of radio spectrum in the 1.5 GHz to 50 GHz range [34].

A microwave link requires the installation of a microwave dish at either end of the link, with a clear line of sight between the two dishes. The distance a microwave link can cover is highly dependent on the frequency used to transmit the data signal, the size of the dishes used, and the ability to achieve a clear line of sight between the transponders. This often requires the use of large poles or towers to mount the microwave dishes.

The microwave link propagation characteristics depend on topographic and atmospheric conditions such as high humidity, rain and smoke. For example, microwave radio propagation is impacted by large bodies of water that can modulate signals in unfavourable ways.

Satellite technologies may also be used to provide backhaul services, and is the only option for the 72.7% of the landmass that is not covered by terrestrial mobile wireless networks. Satellite technologies have limited capacity, suffer from latency and are affected by atmospheric conditions such as heavy cloud cover and smoke. However next generation satellite services will provide capabilities, including addressing issues such as latency.

3.6 The National Broadband Network

In April 2009 the Australian Government announced that it will roll out the National Broadband Network (NBN) to Australian homes, schools and businesses. NBNCo was established to rollout a FTTP network to 93% of Australian premises, with the remaining 7% to be serviced by next generation satellite and fixed wireless technologies.

The NBN FTTP network will initially offer maximum data rates of 100 Mbps in the downlink and 40 Mbps in the uplink via its FTTP network. NBNCo have also stated that they will offer a 1 Gbps downlink and 400 Mbps uplink service by 2014[35]. The fixed wireless service will make use of LTE technology and will initially offer peak download speeds of 12 Mbps, with faster speeds being made available into the future[36]. The current, interim satellite services offered by NBN Co are capable of peak download speeds up to 6 Mbps, however the company intends to launch two satellites in 2015 that will enable downloads speeds of up to 12Mbps[37].

In a global context the rollout of a network on the size and scale of the NBN is unique. It will enable coverage across all of the Australian landmass. Additionally, the way the network is being rolled out provides a unique opportunity for the Australian environment. The NBN infrastructure includes rolling out Network Termination Device (NTDs) to each premises, which provides the termination point for the network. Each NTD includes four Ethernet ports, which could in theory enable four different providers to connect to individual premises. This technology is likely to underpin innovation in the delivery of future broadband applications and services, and could provide a unique opportunity for Australian PSAs, that is unavailable in many other countries, to improve their communications in a way that adds capacity, redundancy and resilience. This is explored further in the following section.

4 Options for PSA Broadband Application Delivery

There are several technologies that are available today, or will be available in the near future, that can enable the provision of mobile broadband applications for PSAs. This section introduces these technologies, which are based on the available broadband access technologies defined in Section 3.

The technologies are split into:

- ***Broadband access technologies*** that connect end-user devices and applications to a broadband network; and
- ***Local backhaul*** that may be required to connect the broadband access technologies into the backhaul network. .

These technologies are described below.

4.1 Broadband Access Technologies

This section describes the broadband access technologies that may be used by PSAs in business-as-usual cases, as well as incidents at major venues and random locations.

4.1.1 Dedicated PSA LTE Network Access

A dedicated PSA LTE network will provide a single telecommunications platform to handle PSA communications, offering a high level of security and capacity in coverage areas subject to the capacity of the network.

The advantage of a dedicated PSA LTE network is that it facilitates 'anytime, anywhere' access for mobile PSA units within the coverage area. In addition, a dedicated PSA LTE network could assist with streamlining coordination and information sharing across different PSA organisations, including across state boundaries, for example in disaster relief efforts.

The recent ACMA announcement that 5+5MHz of spectrum has been set aside for the PSAs, creates the opportunity for the state and territories to establish a harmonised and dedicated PSA LTE network across the country[38]. This is consistent with the 2010 Federal Communications Commission (USA) white paper "*The Public Safety Nationwide Interoperable Broadband Network: A New Model for Capacity, Performance and Cost*" and is likely to cater for business as usual applications into the future[39]. A dedicated LTE network that makes use of this spectrum would be capable of supporting downlink speeds in the order of 10 Mbps per user today, with the potential to increase to around 12.5 Mbps per cell by 2015 based on future upgrades of LTE equipment[40].

Whilst it could be argued that PSAs require more spectrum for their communication needs, this does not take into account how an LTE network would most effectively be deployed. Whilst the allocation of more spectrum could enable faster speeds with the deployment of fewer base station sites it reduces the resiliency of the network and is highly undesirable for PSA communications. By deploying a larger number of base station sites, faster communications will be achieved. However, more importantly, sufficient base station density will also enable the network to self optimise during a period of high demand or when there is a base station outage, enabling base stations to dynamically handover users to neighbouring sites when required[41]. This provides valuable resilience to a network with a dense deployment of base stations because in the event of an outage a small, localised black spot will result and self-optimisation will enable adjacent base station sites to fill these black spots until the damaged base station is restored. Conversely, in the event of an outage in a network with fewer base station sites a large blackspot will result and dynamic self-optimisation may not be an option, resulting in an inability to communicate.

While deployment of a dedicated PSA LTE network with dense base station coverage is important to cater for the PSA business as usual activities in the metropolitan areas and major regional centres, the deployment of such a network to meet these needs in all rural and remote areas and to support incidents at major venues in metro centres is unfeasible due to the following:

- Firstly, and most importantly, relying on a single dedicated network reduces the redundancy and resilience of PSA communications. For example, if a bushfire were to render a base station useless, all PSA communications in that area would be impacted, especially if self-optimisation was not available.

- Secondly, the PSA LTE network could not cover 100% of the Australian landmass. As discussed in Section 3.2.1, commercial providers coverage is in total around 27.3% of the landmass, and it is unlikely that a PSA network would meet the coverage and capacity of these networks.

- Thirdly, related to the above point, the cost to build a dedicated PSA LTE network that would provide the necessary coverage footprint and capacity in all metropolitan and rural areas would be very expensive. Telstra spent over $1 billion building the Next G network that initially covered 98.8% of the population or around 27.3% of the Australian landmass[42,43]. Furthermore, it is likely that the cost to deploy a new dedicated PSA LTE network would be higher as the commercial providers were able to reuse the prime antenna locations they currently occupied with existing network infrastructure. As these sites are mostly occupied, the PSA LTE network deployment would be less than optimal and could have a smaller coverage footprint than the commercial carriers. Alternatively greater investment in infrastructure will be required.

- Fourth, if additional spectrum were allocated for a national dedicated PSA LTE network this would result in inefficient use of finite and precious resources, namely spectrum, since the network would be over engineered to cater for incidents at major venues and random locations, which are considered to be rare and whose location is unknown in advance.

- Fifth, a dedicated LTE network may not be able to cater for the bandwidth demands of PSAs into the future, even with planned upgrades for additional network capacity and irrespective of the amount of spectrum available. This means that PSAs must consider alternative options to augment their capacity no matter what the capability of their network is.

- Lastly, as discussed in Section 3.2, mobile broadband speeds are impacted by a number of factors including uncontrollable end-user constraints such as location, which may not allow for a high quality line of sight transmission between end-user equipment and the base station. This could result in unreliability of the dedicated PSA LTE network, for example call drops outs may be experienced. It would be unwise for PSAs to rely on a single network for communications.

Alternate technologies for broadband access need to be available to PSAs to augment the network coverage and capacity of a dedicated LTE network and to provide redundancy and reliability in the form of alternative transmission paths, especially for incidents at major venues and random locations where PSA broadband demands are likely to be higher than business-as-usual. Alternative broadband solutions that complement a dedicated PSA LTE network may also reduce the cost of establishing national communications infrastructure that meets PSA requirements under all circumstances.

There are a number of different options for augmenting a dedicated PSA network for incidents at major venues and random locations. Data and communications requirements for major venues can be forecast in advance enabling additional and alternative infrastructure to be deployed ahead of time that can be used by PSAs in the event of an incident. This network infrastructure could be a permanent deployment used for multiple events at the same location throughout the year, or be temporarily deployed ahead of time for a particular event. Conversely incidents at random locations may occur where there is limited communications infrastructure, meaning new network links may have to be quickly established to cater for PSA bandwidth demands following an incident.

The following sections discuss the various options that are available for PSAs to augment the coverage and capacity of a dedicated PSA LTE network and importantly provide a further level of redundancy and resilience during incidents at major venues and random locations.

4.1.2 LTE Roaming on commercial networks

As noted in Section 4.1.1, it is unachievable for PSAs to build a dedicated LTE network that covers 100% of the Australian landmass, and it is also unlikely that the PSA network will have the equivalent coverage and capacity as the commercial carriers described in Section 3.2.1. It is therefore essential the PSA's have in place a roaming agreement with at least one commercial carrier to extend and augment their network coverage.

Roaming agreements with commercial carriers have the benefit of providing additional LTE capacity, redundancy and reliability to PSA communications.

Roaming onto commercial networks could, in theory, increase the available bandwidth capacity by more than twice that enabled over a dedicated PSA network. It would also increase the reliability of PSA communication strategy by providing a redundant communications platform to fall back on should there be an outage on the dedicated PSA LTE network. Commercial carriers also have the added redundancy of multiple wireless network platforms to fall back on. For example, if there is an outage on the carriers LTE network, the user terminals will fall back onto their 3G network in order to maintain communications. This could mean that PSAs not only have access to the commercial carrier's LTE network, but also their 3G network. Commercial roaming agreements may also reduce the cost of rolling out a dedicated PSA LTE network by reducing the area the dedicated PSA network is required to cover, instead leveraging existing coverage of commercial network.

The capability to roam onto a third party network would require the dedicated PSA network operator to formally partner with at least one of the domestic LTE or 3G mobile wireless carriers. The partnering agreement would establish the framework under which PSA end-user equipment could access the third party network infrastructure. It would require some integration of the PSAs core network infrastructure with the commercial carrier's infrastructure. This type of roaming arrangement has been implemented in the United States of America by a partnership between Verizon, Motorola and Ericsson[44,45]. It could be encouraged in Australia, by making this a requirement for commercial networks to provide when bidding for spectrum.

Another requirement of any roaming agreement would be the capability to encrypt PSA communications on the commercial carrier's network to ensure secure communications between PSA personnel. PSA traffic can be prioritised over general traffic on these networks. This would be highly desirable in areas the dedicated PSA network did not cover and in particular during incidents where PSA broadband demands may be high. The security of LTE roaming would be at the same level as the dedicated LTE network.

The ability of PSA users to roam onto commercial networks will impact the performance of these networks for public users. It is important that the general public is able to maintain the ability to make calls and in particular calls to emergency numbers such as 000 so that they are able to both request assistance and potentially assist PSAs by providing on the ground information during an incident. Therefore completely prioritising all forms of PSA traffic over public traffic is not desirable or feasible, so careful planning would be required to determine what PSA services are prioritised over general use and under what scenarios.

To address some of these issues, two separate roaming agreements could be agreed between PSAs and commercial operators. One roaming arrangement could be for business-as-usual scenarios where PSA users roam onto the commercial network when they are outside the dedicated PSA network coverage. In this scenario PSA applications could be given limited prioritsation. Importantly, this arrangement should not negatively impact the public users network access or experience as it is anticipated that there would only be a small number of PSA users trying to access a given base station at any one time.

A second roaming arrangement could be made to plan for incidents at random locations where the PSA users are given more network resources and higher prioritsation, while the general public access to the network is limited to voice calls only. PSA users in this scenario may be using the PSA network for their primary communications while the commercial network is used to cater for the additional broadband requirements created by the larger concentration of PSA users.

4.1.3 Portable LTE Access (CoWs)

During incidents at major venues and random locations PSA demands for broadband services are likely to be high and this will put a strain on the existing network resources of a dedicated PSA network. One way to overcome this shortfall of available capacity is to deploy a Cell on Wheels (CoW). CoWs are generally trailer-mounted enclosures or converted shipping containers which house base station equipment and a mast, which can be winched up to support an antenna. The level of network security would be the same as the dedicated PSA LTE network once operational.

CoWs can be used in different ways to augment existing coverage or provide access in areas without coverage, depending on the local backhaul technology that is used to connect the CoW into the telecommunications network. The additional capacity provided by a CoW could be as much as 100% that of a dedicated PSA LTE network, if an independent local backhaul solution is used. This scenario would also provide redundancy to the dedicated PSA LTE network. However, if the CoW uses the dedicated PSA LTE network to connect back into the telecommunications, no additional capacity or redundancy may be achieved. Local backhaul solutions are discussed further in Section 4.2.

Portable wireless CoWs are commonly deployed by commercial networks to augment their existing network coverage and capacity during incidents at major venues such as music festivals and major sporting events. As incidents at major venues typically occur annually in the same location, the transmission equipment and access points required to provide connectivity back into the carrier's network are generally well established.

CoWs could also be deployed by PSAs to provide coverage when there are incidents at random locations such as the Queensland floods and Victorian bushfires. During these incidents the existing network infrastructure may be damaged and unable to provide coverage, or be in an area with limited existing coverage. In these situations the CoWs would be deployed to fill in the network black spots.

CoWs may take some time to deploy, so careful planning is required to ensure there are sufficient numbers of them to deploy across any jurisdiction, enabling them to be deployed quickly in response to an incident.

4.1.4 Local WiFi Access

In some areas where a large number of people congregate, the use of dedicated WiFi hotspots may provide a suitable access technology for PSAs. This would be an appropriate technology to consider for major venues such as sporting facilities and public spaces, for example Melbourne's Federation Square. Dedicated WiFi hotspots may also be useful in areas where large numbers of people transit including major metropolitan train stations, shopping centres and city high streets.

A recent decision by the ACMA has made available 50 MHz of spectrum in the 4.9 GHz band for use by PSAs[46]. This would be ideal spectrum for high-capacity and short-range communications enabled by WiFi hotspots. While use of lower spectrum bands such as the 2.4 GHz band enables better penetration of building structures to provide a larger coverage area when used indoors, higher spectrum bands such as the 4.9 MHz band enable higher data rates. An additional advantage of the 4.9 MHz band is that it is dedicated for PSA use only, and therefore less prone to interference from other devices and more likely to support data rates closer to those demonstrated under ideal conditions.

The additional capacity provided by a local WiFi hotspot could be significant, depending on the local backhaul technology that connects the WiFi router to the telecommunications network. As noted in Section 3.3, WiFi routers are now capable of transmitting broadband speeds of up to 300 Mbps over distances of up to 450m in ideal circumstances. The additional capacity could provide greater scope for use of multiple high bandwidth applications by PSAs within a small area. Additional local WiFi access could be used to add redundancy to the PSA network if an independent local backhaul solution is used, as communications would not be dependent on a single dedicated LTE network.

The installation of local WiFi hotspots in areas where incidents at major venues occur would provide additional capacity and redundancy to cope with potentially high PSA broadband demands. WiFi hotspots may also reduce the cost of a dedicated PSA LTE network deployment, by reducing the need to design the network to cope with high bandwidths in areas where PSA communication demands may be high, for example at major venues.

Dedicated WiFi hotspots may not be useful for incidents at random locations depending on their location, as pre-installation is assumed. Further disadvantages of dedicated WiFi hotspots is that the coverage area is small compared to a LTE network, and handover between hotspots and onto the dedicated PSA LTE network would need to be carefully engineered. Low signal strengths can limit the performance of a WiFi hotspot, and transmission within buildings can be difficult as WiFi signals are susceptible to interference and absorption effects.

4.1.5 Portable WiFi Hot Spots

Portable WiFi Hot Spots refers to the placement of WiFi routers in PSA vehicles, which may be activated once stationary providing there is access to a suitable local backhaul technology. These are referred here on in as WiFi on Wheels (WoWs).

Like local WiFi access, WoWs would use the 4.9 GHz band that has been allocated to PSAs by the ACMA. This would be ideal spectrum for high-capacity and short-range communications enabled by WiFi hotspots.

WoWs could be quickly established by PSAs to provide enhanced communications over and above a dedicated LTE network, in particular during incidents at random locations. As with dedicated WiFi hotspots, significant additional capacity as well as redundancy could be made available for PSA use, depending on the local backhaul technology.

The disadvantage of WoWs for PSAs could be the time taken to establish the local backhaul connection into the broader telecommunications network. As with dedicated WiFi hotspots, the quality of WoWs will be dependent on factors such as the coverage area, building penetration and best efforts service.

4.1.6 Fixed Ethernet

While it is recognised that the vast majority of applications used by PSAs require mobility, in some cases fixed Ethernet access may be an appropriate access technology. An Ethernet connection could be used to directly connect a PSA technology (such as a computer on board a vehicle) into a fixed telecommunications network. This could provide a suitable access technology for a temporary incident control station where data is aggregated, decision making occurs and instructions are communicated to PSA personnel, or for providing data access over a duration of time at a fixed location (for example, an ambulance attending an incident that may take some hours before a patient may be moved).

In this report two fixed Ethernet options are considered:

- “Fourth Port” on a NBN NTU, which is discussed further in Section 4.2.4.
- A Data Hydrant, which is discussed further in Section 4.2.5.

Both of these options could be facilitated by the NBN, and could provide Australian PSAs with a unique opportunity that is unavailable in many other countries. Both options would provide redundancy as well as enhanced reliability, as fixed networks are less prone to ‘drop-outs’. Another advantage of fixed Ethernet access is that quality of service can be guaranteed, and the additional capacity provided is significant, for example over the NBN speeds in the order of 100 Mbps would be available today, rising to 1 Gbps by 2014. The greatest disadvantages of the fixed Ethernet access are the lack of mobility and the limited number of access points, hence this technology is only suitable for a limited number of applications.

4.1.7 Satellite Access

As noted in section 4.1.1, the size of the Australian continent makes it impractical to rollout a dedicated LTE network that covers 100% of the landmass. To date Australia’s largest mobile wireless network only covers about 27.3% of the landmass, leaving about 72.7% without any form of terrestrial mobile wireless access. In these areas the only broadband access technology available to PSA personnel is satellite communications. The advantages and disadvantages of satellite technologies are discussed in Section 3.2.

4.2 Local Backhaul

A dedicated or commercial LTE network, fixed Ethernet access and satellite services have direct connections into a telecommunications network, either through existing backhaul or the NBN. However, mobile LTE access (CoWs), and dedicated and mobile local wireless access technologies all require local backhaul solutions to connect the access technology into the national telecommunications network. For each of these technologies several local backhaul options exist, and these are discussed below.

4.2.1 LTE relay over dedicated PSA networks

LTE networks can be used to provide local backhaul as shown in Figure 4 by connecting a CoW to a base station with high capacity backhaul. This is known as LTE relay. The LTE CoW has an LTE terminal that receives the base station signal and retransmits it locally. End user devices communicate with the LTE CoW, which then transmits the signal back to the LTE base station. LTE relay ideally requires the two base stations to have direct line of sight. The distance provided by a LTE relay hop is dependent on the spectrum used and as with LTE wireless mobile may vary from a few hundred metres up to 200km.

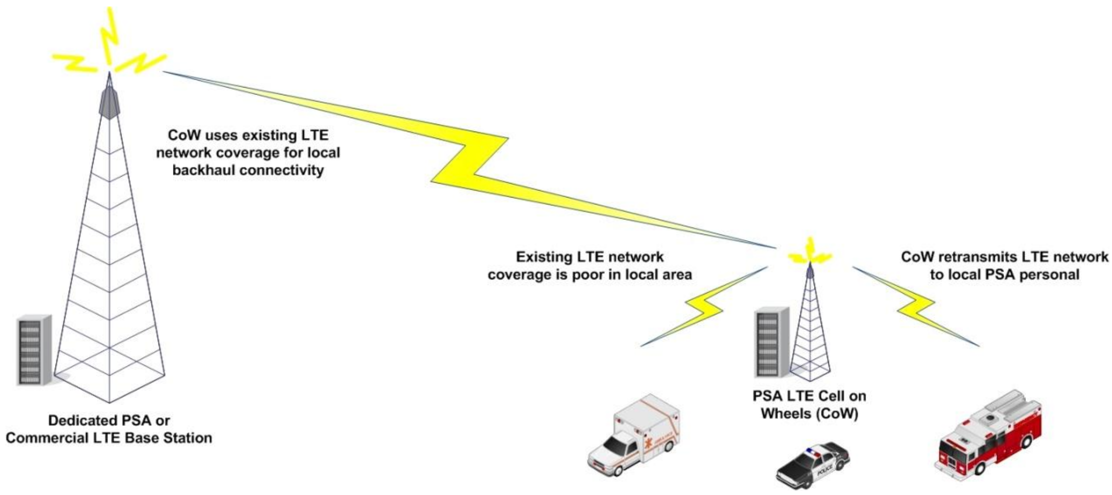


Figure 5: LTE relay

LTE relay over a dedicated PSA LTE network provides a way to temporarily extend the coverage of an existing base station to an area that has low signal strength. It does not provide any additional capacity or redundancy over and above the dedicated PSA network as it reuses the resources of this network locally.

The advantage of using LTE relay over a dedicated PSA network is that links can be established quickly, making it useful for incidents at random locations. The disadvantage of LTE relay over a dedicated PSA network is that it reduces the overall capacity of the PSA transponder on a base station, and may impact on the delivery of other PSA applications.

4.2.2 LTE relay over commercial networks

LTE relay using a commercial carrier's network works in the same way as LTE relay over the PSA's LTE network, and can be used to connect CoWs into the telecommunications network. The major difference being that it requires a formal roaming agreement between the PSAs and the commercial network operator to connect to the base station. To allow access to the commercial carrier network, the PSA network would need to have pre-existing network infrastructure interconnected with the commercial carrier's network. Hence this type of local backhaul is only an option if a general LTE roaming agreement is in place.

The same advantages and disadvantages apply to commercial LTE relay as to a LTE relay over a dedicated PSA network. Additional advantages of commercial network LTE relay include the increase in coverage and capacity as PSAs have access to third party transponders in addition to their own. This also adds redundancy, as there is the option of moving onto the commercial carrier's network if there is an outage on the PSA network.

4.2.3 Wireless Local Loop

Wireless Local Loop (WLL) technology is a data and voice gateway that uses a mobile network as a connection back into the telecommunications network in a similar way to LTE relay. WLL is also referred to as fixed wireless access and is currently used in Australia to provide a traditional telephone service via the Telstra NextG network where it is too expensive or too difficult to deploy a copper twisted pair telephone line, as well as by NBN Co as its wireless solution. The latest WLL terminals have the option of integrated WiFi so can accommodate both a physical Ethernet connection or a wireless connection without needing any additional equipment[47].

WLL would be used in conjunction by PSAs to connect a WoW into the network with LTE access, communicating either directly with the dedicated PSA network, commercial network or via a CoW. Depending on the mobile wireless local backhaul chosen, additional redundancy and capacity may be provided.

WLL terminals have the same advantage as LTE relay in their ability to be quickly deployed in response to a major incident at a random location. WLL terminals also share the disadvantages as LTE relay in consuming the overall available bandwidth of the serving LTE network and requiring a pre-established roaming agreement when a commercial carrier's network is used for connectivity.

4.2.4 Fourth port PSA network access

As discussed in Section 3.6 the rollout of the NBN in Australia has created a unique opportunity for Australian PSAs to build a world leading communications network to augment the PSA LTE network, that is unavailable in many other countries. One example of how the NBN could be leveraged is through PSAs arranging access to the "Fourth Port" on NBN NTUs to achieve an exclusive high-speed fixed Ethernet broadband connection from almost any building in the country[2]. This Fourth Port will have the capacity to deliver much higher data rates than would be possible over a dedicated LTE network, with the fibre fed ports able to deliver 100 Mbps today with the potential to deliver 1 Gbps/400 Mbps downlink/uplink and higher in the future.

Fixed technologies will be capable of providing a more predictable and potentially higher level of service compared to wireless or satellite technologies. Hence, the NBN Fourth Port would provide the perfect local backhaul solution when deploying WoWs or LTE CoWs at major venues such as music festivals or sporting events. These dedicated ports could also be used during incidents at random locations when setting up field incident control headquarters and to provide backhaul connectivity for WoWs and LTE CoWs. However, it should be noted that without a WoW or a CoW, Fourth Ports are only capable of providing fixed Ethernet services, which do not provide mobility and would only be available at fixed premises.

Advantages of using the Fourth Port as a local backhaul technology where possible include an ability to rapidly configure additional services, compared to other local backhaul solutions such as microwave (discussed in Section 4.2.6), as well as freeing up valuable capacity on the dedicated PSA LTE network to support additional bandwidth capabilities over and above business-as-usual usage. For example, Fourth Port connections could be used for high capacity, low latency applications and the dedicated LTE network could be used for mobile applications. This solution would add redundancy to the PSA communications network. In addition, this would add reliability to communications, given the stability of fixed networks. It would take advantage of the unique position provided by the NBN rollout and could position Australia as a world leader in emergency services communications.

The use of fourth ports may have minimal additional costs to PSAs over and above the dedicated PSA LTE network rollout, as the NBN is already being rolled out by the Australian Government. It may also allow a for reduced cost rollout of the dedicated PSA LTE network, as this network would not have to be over-engineered, as high bandwidth applications could be implemented using WoWs with Fourth Port local backhaul access.

Discussion would be required with NBN Co regarding the feasibility of deploying these solutions and other related issues, such as rollout times, costs and encryption. Additionally, NBN Co may not be able to offer the service themselves given separation undertakings. A third party RSP may need to be introduced.

[2] We would recommend that the Fourth Port is always used, so there would be no confusion by PSA personnel who may need to quickly establish a connection over the NBN.

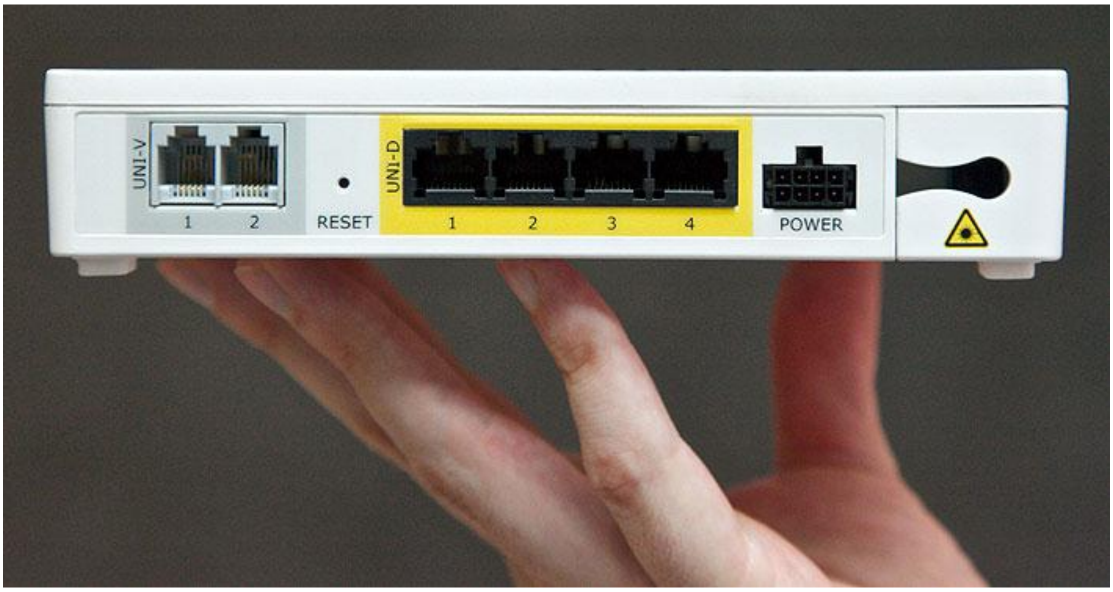


Figure 4:NBN Co NTUs have four ports, of which one could be used for PSA communications[48].

4.2.5 Data Hydrants

Data hydrants are dedicated access points to a fixed Ethernet connection at easily accessible locations for exclusive use by PSAs, separate to NBN access at buildings as described in Section 4.2.4. For example, data hydrants could be located in close proximity to existing water hydrants that are available for firefighting services in metropolitan areas. They could also be established in areas where PSA activity could be high, for example outside major venues.

Data hydrants could be provided by NBN Co, through the provision of additional dedicated access points for PSAs. They may also be supplied by other telecommunications providers with fibre networks, for example Telstra, Optus or NextGen Network amongst others. Discussion would be required with providers regarding the feasibility of deploying these solutions and other related issues, such as rollout times, costs and encryption.

Data hydrants have the same advantages and disadvantages as Fourth Port access, including providing redundancy and reliability through a more predictable and potentially higher level of service compared to other technologies; enabling the ability to rapidly configure additional services compared to other local backhaul solutions such as microwave; and freeing up capacity on the dedicated PSA LTE network to support additional bandwidth capabilities over and above business-as-usual usage. However, additional advantages of data hydrants include that they could make use of point-to-point optic fibre technology rather that GPON, meaning broadband speeds in excess of 10 Gbps could be easily achieved. The requirements for this over and above a 10 Gbps GPON link would need to be established, and may not be required. Data hydrants would also have the advantage of being installed in locations that are easily accessible and well known to PSAs, including in at major venues. Special casings may be required.

Figure 5: Data hydrants could be collocated with water hydrants for PSA access

Data Hydrants do not enable mobility, unless they are used as a local backhaul solution for a CoW or a WoW. They would also only be available at a limited number of locations, agreed by PSAs and the commercial providers.

Because the deployment of Data Hydrants would be specifically for PSAs, there may be an associated deployment cost, however this would be much lower than the costs of rolling out a dedicated PSA LTE network. As with Fourth Port access, Data Hydrants may also allow a for reduced cost rollout of the dedicated PSA LTE network as this network would not have to be over-engineered.

4.2.6 Microwave radio

Microwave networks can be used to provide a local backhaul solution for local WiFi access, WoWs or LTE CoWs. Microwave links can also be deployed as a failover transmission path to complement existing infrastructure where redundancy is required.

Advantages of microwave transmission links include that they are easy to deploy and very portable. The use of smaller microwave dishes makes them easy to include in the standard equipment allocation for WoWs and CoWs.

Disadvantages of using microwave transmission include the time it takes to plan the link including link budgets and license applications as well as the requirement for line of sight transmission. Microwave links are also prone to degradation from atmospheric conditions such as humidity, rain and smoke.

4.2.7 Satellite

As noted in Section 3.5 satellite could be used as a local backhaul solution, to provide a data connection between a remote location and a ground station where terrestrial broadband is unavailable. Satellite local backhaul is the only option for the 72.7% of the Australian landmass that is not covered by terrestrial broadband. One disadvantage of satellite backhaul is its limited capacity, which may prevent the use of some high bandwidth applications. Satellite services also suffer from latency and are heavily affected by atmospheric conditions, such as heavy cloud or smoke cover.

4.3 Choosing the right network solutions

There are a number of options available for PSA communications, that would augment a dedicated PSA LTE network, providing additional redundancy, capacity and reliability where needed. These are summarised in Table 1.

The combination of broadband options used would vary between different incidents at major venues as well as for unincidents at major venues and different combinations of broadband technologies appropriate to PSAs need to be considered further.

In addition PSAs would need to make sure that their equipment was able to operate across multiple technology platforms, for example moving off an LTE network and onto a WiFi network when one becomes available so the LTE network resources are available to those that cannot access the local WiFi network. This would need to happen without a discernable disruption to the user so it is essential that all of these network platforms are built with interoperability in mind. This approach is currently used by commercial carriers to free up resources on their networks since most devices such as smartphones and laptop computers have the capability to operate across different platforms.

Broadband access technology	Local backhaul	Indicative additional capacity by 2015	Incidents at Major Venues	Incidents at Random Locations	Comments
Dedicated PSA LTE Access	Not required as backhaul will be established	n/a	Yes	Yes	A dedicated PSA network would be used for business-as-usual operations, and would be the primary network for PSA voice communications, and potentially other applications, for incidents at major venues and random locations that occur where network coverage is available.
LTE Roaming on commercial networks	Not required as backhaul will be established	300 Mbps	Yes	Yes	Used to provide coverage in areas without PSA network coverage, or augment PSA network capabilities to support high broadband demands. Requires pre-planning and agreements to be in place with commercial operators.
Mobile LTE Access (COWs)	Fourth Port NBN Connection or a Data Hydrant	300 Mbps per CoW	Yes	Yes	Used to provide redundancy in communications and increase broadband capacity. Preferred CoW solution if available due to additional capacity and redundancy.
	LTE relay on PSA network	Reduced PSA network capacity for other PSA access seekers	Not recommended	Yes	Maybe be used to extend PSA coverage in blackspots, or replace damaged PSA network equipment in emergencies e.g following a fire. However, reduces PSA network capabilities.
	LTE relay on commercial networks	300 Mbps	Not recommended	Yes	Used to provide redundancy in communications and increase broadband capacity. Will reduce capabilities of commercial networks for general use.
	Microwave	150 Mbps	Yes	Yes	Used to provide redundancy in communications and increase broadband capacity. Requires line of sight for microwave communications, and this could lead to lengthy set-up times to establish local backhaul
	Satellite	12 Mpbs	For use in	Only option	Used to provide redundancy in communications,

			remote areas only	for 72.7% landmass	especially in remote locations. Satellite backhaul has limited bandwidth capabilities compared to other options.
Dedicated WiFi Access	Fourth Port NBN Connection or a Data Hydrant	300 Mbps per connection	Yes	Yes	Used to provide redundancy in communications and increase broadband capacity. Preferred dedicated WiFi Access solution due to additional capacity and redundancy. Assume established in advance of an incident
	Wireless Local Loop (WLL) on PSA network	Reduced PSA network capacity for other PSA access seekers	Not recommended	Yes	Maybe be used to extend PSA coverage in blackspots, or replace damaged PSA network equipment in emergencies e.g following a fire. However, reduces PSA network capabilities.
	Wireless Local Loop (WLL) on commercial networks	300 Mbps	Not recommended	Yes	Used to provide redundancy in communications and increase broadband capacity. Will reduce capabilities of commercial networks for general use.
	Microwave	150 Mbps	Yes	Yes	Used to provide redundancy in communications and increase broadband capacity. Requires line of sight for microwave communications, and this could lead to lengthy set-up times to establish local backhaul
	Satellite	12 Mpbs	For use in remote areas only	Only option for 72.7% landmass	Used to provide redundancy in communications, especially in remote locations. Satellite backhaul has limited bandwidth capabilities compared to other options.
Portable WiFi (WoWs)	Fourth Port NBN Connection or a Data Hydrant	300 Mbps per connection	Not recommended (assume pre-planning and dedicated WiFi)	Yes	Used to provide redundancy in communications and increase broadband capacity. Preferred WoW solution if available due to additional capacity and redundancy.
	Wireless Local	Reduced PSA network	Yes	Yes	Maybe be used to extend PSA coverage in blackspots,

	Loop (WLL) on PSA network	capacity for other PSA access seekers			or replace damaged PSA network equipment in emergencies e.g following a fire. However, may reduce PSA network capabilities.
	Wireless Local Loop (WLL) on commercial networks	300 Mbps	Yes	Yes	Used to provide redundancy in communications and increase broadband capacity. Will reduce capabilities of commercial networks for general use.
	Microwave	150 Mbps	Yes	Yes	Used to provide redundancy in communications and increase broadband capacity. Requires line of sight for microwave communications, and this could lead to lengthy set-up times to establish local backhaul.
	Satellite	12 Mpbs	For use in remote areas only	Only option for 72.7% landmass	Used to provide redundancy in communications, especially in remote locations. Satellite backhaul has limited bandwidth capabilities compared to other options.
Fixed Ethernet	Fourth Port NBN Connection	1 Gbps per connection	Yes	Yes	Used to provide redundancy in communications and increase broadband capacity. Lacks mobility so only useful in a limited number of scenarios.
	Data Hydrant	> 10 Gbps, subject to deployment scenario	Yes	Yes	Used to provide redundancy in communications and increase broadband capacity. Lacks mobility so only useful in a limited number of scenarios.
Satellite services	Not required as backhaul will be established	12 Mbps	For use in remote areas only	Only option for 72.7% landmass	Only option for 72.7% landmass not covered by terrestrial mobile broadband networks.

Table 1: Summary of Broadband options for PSAs

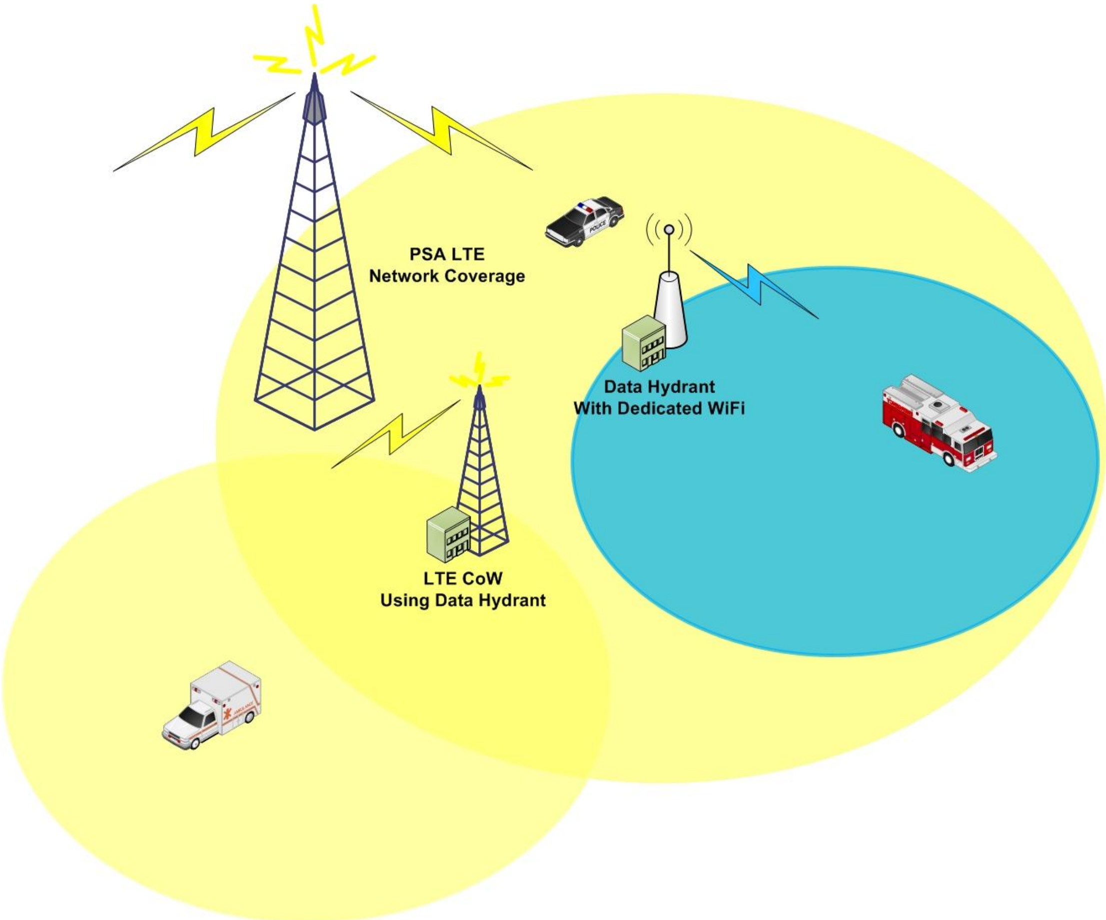


Figure 6: An example of a communications network for use in the event of an incident at a major venue.

Figure 6 shows an example combination of broadband technologies that could be used in major venue, for example at a sport stadium. The dedicated PSA LTE network would provide coverage over the area, and could be used for voice communications in the event of an incident. A CoW could be established via a Data Hydrant to provide additional capacity and to extend the coverage of the LTE network, to make sure the entire venue had coverage. WoWs could be pre-established, connected to data hydrants at the venue, to provide additional capacity and redundancy. These WiFi hotspots could be used to transmit high broadband applications such as video communications.

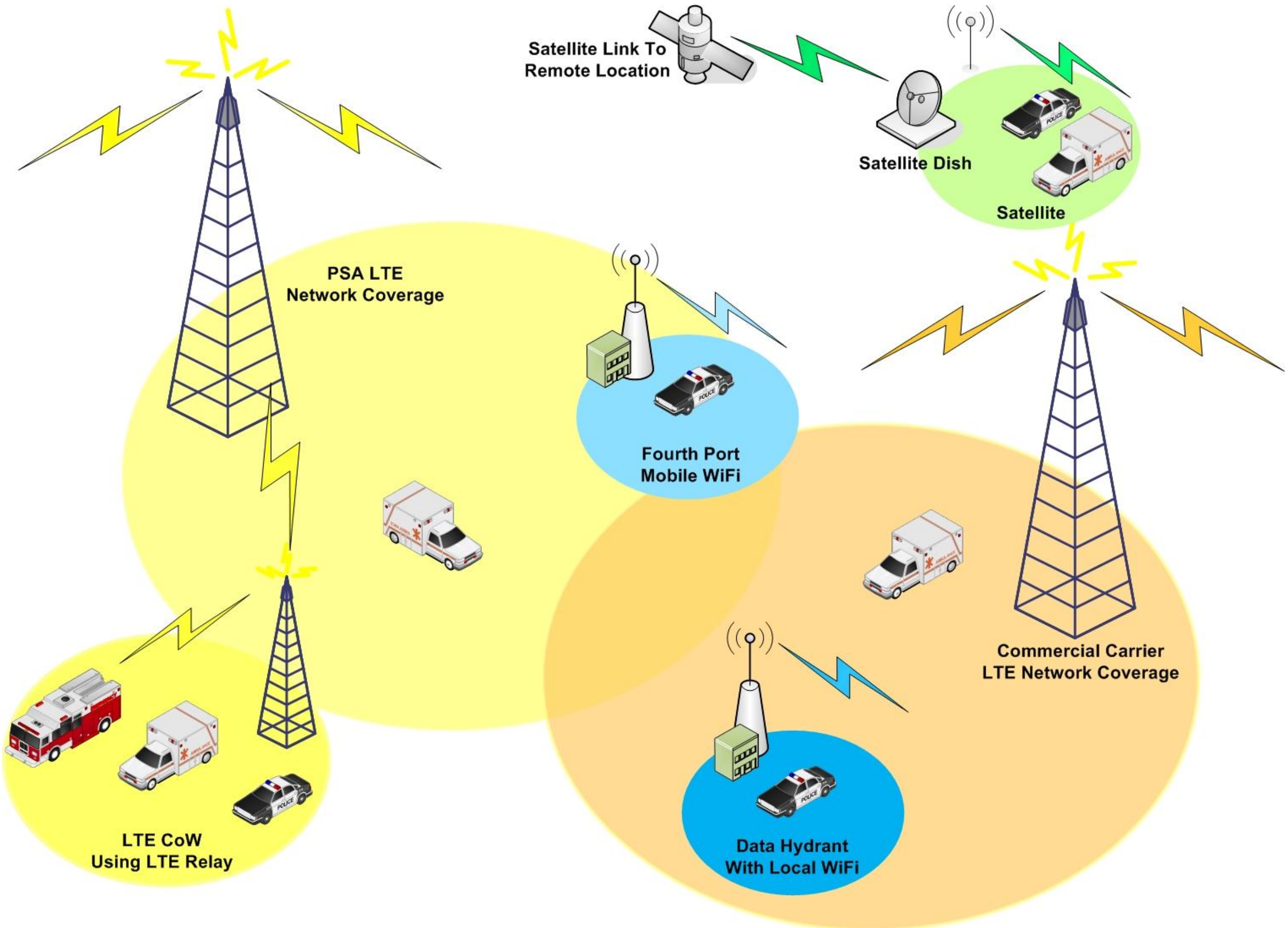


Figure 7: Example of broadband technologies for use in an incident at a random location.

Figure 7 shows an example combination of broadband technologies that could be used at an incident at a random location, for example a natural disaster across a large area. The dedicated PSA LTE network would provide coverage over some of the affected area but not all. To extend the coverage of PSA communications could make use of a commercial network with wider coverage area, as well as CoWs that connect via LTE relay to the PSA network. WiFi hotspots could be established either at data hydrants, or by making use of the fourth ports on buildings in the affected area. Voice communications could occur over the mobile wireless broadband solutions, while the local wireless access solutions can provide additional capacity to transmit high bandwidth applications such as video content. Satellite communications can be used for areas where no terrestrial solution is available.

5 Conclusion

In the future PSAs are likely to make use of an increasing number of broadband applications to support their decision-making and responses to business-as-usual, as well as incidents at major venues and random locations. Low bandwidth applications such as voice communications and Push-to-Talk capabilities will continue to be commonly used. A range of other technologies will be increasingly used to respond to incidents including video conferencing and streaming, remote sensing, cloud computing and database access and image transfers. Newer technologies such as augmented reality and robotics will also have an important role to play in PSA responses into the future. The increased use of these broadband applications will drive increasing demands for high-speed broadband access.

A dedicated PSA LTE network with 5+5 MHz spectrum will cater for business-as-usual use by PSAs, and help streamline communications across different agencies including across interstate borders. It is an appropriate technology providing mobility within network coverage areas. However, a dedicated PSA LTE network will not cover 100% of the Australian landmass and will be unable to cater for high broadband usage, as is expected to be required for incidents at major venues and random locations, regardless of the amount of spectrum that is made available.

Additional delivery options for PSA broadband access should be explored, not only to provide additional broadband capacity during incidents at major venues and random locations to enable traffic offloading from the dedicated PSA LTE network , but also to provide redundancy (and therefore potentially improve reliability) of PSA communications networks.

A number of broadband access options exist for PSA use, to augment the facilities provided by a dedicated PSA LTE network. Roaming onto commercial LTE networks will enable PSA network coverage to be extended in areas where coverage is limited, and provide redundancy and additional capacity, and increase resilience. It also provides a 'quick to market' approach while a dedicated PSA network is established. It is recommended that partnering agreements are established quickly between PSA network operator(s) and at least one commercial network operator.

The use of CoWs and local WiFi networks, either dedicated or portable, also provide a way of increasing capacity in local areas. CoWs are useful to extend PSA LTE coverage for incidents at major venues or as emergency replacements for PSA LTE network equipment. WiFi networks can be used to provide increased capacity during incidents at major venues or in areas where there is a high throughput of people on a regular basis, in which case dedicated hotspots would be recommended. WoWs can be used in incidents at random locations, where dedicated hotspots are not already installed. These solutions require a local backhaul solution to connect the WiFi router or CoW into the backhaul telecommunications network. Depending on the local backhaul technology used, additional capacity may be significant. These CoWs and WiFi networks also add a level of resilience and redundancy to the PSA communications network by providing an alternate communications platform in the event of an outage on the PSA LTE network, assuming a different local backhaul technology is used.

Local backhaul technologies include LTE networks, microwave radio and satellite options, which have different applications depending on the use case. However the most efficient local backhaul technology would make use of a Fourth Port or Data Hydrant. Both of these could be enabled by the NBN, and provide a unique opportunity for PSAs that are unavailable in other countries. Both Fourth Port and Data Hydrant access would provide significant additional broadband capacity for PSAs, in addition to network redundancy. Given that the NBN is being rolled out to every home, school and business in the nation, easy access could be facilitated for PSA use in both incidents at major venues and random locations. This provides a unique solution for the Australian environment, and could position the country as a global leader in PSA communications providing enhanced and future-proofed capacity as well as network redundancy and resilience, when used in conjunction with a dedicated PSA LTE network.

Additional work would need to be undertaken to establish the ease at which the different communications options presented in this paper could be effectively used by PSAs, including protocols for establishing communications links over networks that augment the dedicated PSA LTE network.

References

[1] ACMA media release 81/2012 – 29 October: http://acma.gov.au/WEB/STANDARD/pc=PC_600087

[2] GQ-AAS Report: Public Safety Mobile Broadband Demand Requirements (Project 1) Final Report v2.2 pg (publicly available version) 22

[3] http://www.cisco.com/en/US/tech/tk652/tk698/technologies_tech_note09186a0080094ae2.shtml

[4] http://www.skype.com/intl/en/home

[5] http://www.webex.com.au/

[6] http://www.vidyo.com/

[7] http://www.skype.com/intl/en-us/security/detailed-security/

[8] GQ-AAS Report: Public Safety Mobile Broadband Demand Requirements (Project 1) Final Report v2.2 pg 42 (publicly available version)

[9] GQ-AAS Report: Public Safety Mobile Broadband Demand Requirements (Project 1) Final Report v2.2 p37 (publicly available version)

[10] http://www.broadband.unimelb.edu.au/resources/white-paper/2012/Interface-information-interaction.pdf

[11] "A Guide to Broadband Technologies", R. Ayre, K. Hinton, B. Gathercole and K. Cornick, *The Australian Economic Review*, vol. 43, no. 2, pp. 200–8.

[12] Alcatel Lucent Media Release / Website: Turbocharge copper networks to extract more value http://www.alcatel-lucent.com/wireline/copper-access.html

[13] "A Guide to Broadband Technologies", R. Ayre, K. Hinton, B. Gathercole and K. Cornick, *The Australian Economic Review*, vol. 43, no. 2, pp. 200–8.

[14] http://newscenter.verizon.com/press-releases/verizon/2010/Verizon-s-Second-Field-Trial-of-10-Gigabit-per-Second-XG-PON-Fiber-to-the-Premises-System-Affirms-FiOS-Network-Design-Is-Future-Ready.html

[15] NBNCo Corporate Plan 2012-15: http://www.nbnco.com.au/assets/documents/nbn-co-corporate-plan-6-aug-2012.pdf, page 56

[16] Ericsson press release "Ericsson and Telstra achieve world first 200 km cell range in nationwide network with up to 14.4 Mbps": http://www.ericsson.com/kr/ericsson/press/releases/20070212-1104433.shtml

[17] *Where wireless makes sense* http://www.broadband.unimelb.edu.au/engage/pubs/wp/where-wireless-makes-sense-web.pdf

[18] http://www.3gpp.org/HSPA

[19] http://www.3gpp.org/LTE

[20] http://www.telstra.com.au/mobile-phones/coverage-networks/network-information/nextg/index.htm

[21] http://www.optus.com.au/aboutoptus/About%20Optus/Network%20Coverage

[22] http://www.vodafone.com.au/aboutvodafone/network/expansion-plan

[23] http://www.telstra.com.au/mobile-phones/coverage-networks/our-coverage/mobile-broadband/

[24] http://www.vodafone.com.au/aboutvodafone/network/network-evolution

[25] http://www.telstra.com.au/mobile-phones/coverage-networks/network-information/nextg/index.htm

[26] http://compnetworking.about.com/od/routers/gr/belkin-n1.htm

[27] http://www.motorola.com/web/Business/Products/Wireless%20LAN%20Devices/WLAN%20Access%20Points/AP-7131/_Documents/_staticfiles/AP-7131_Spec-Sheet_0910-web.pdf

[28] http://www.motorola.com/web/Business/Products/Wireless%20Broadband%20Networks/Mesh%20Networks/MOTOMESH%20Quattro/Vehicle%20Mounted%20Modem/_Document/_Static%20files/MOTOMESH_Quattro_Overview_Spec_Sheet.pdf

[29] http://www.netgear.com.au/service-provider/products/routers-and-gateways/cable-gateways/CGD24N.aspx#
[30] http://www.acma.gov.au/webwr/_assets/main/lib312061/five-year_spectrum_outlook_2011-2015.pdf page 85
[31] https://acts.grc.nasa.gov/docs/3rdKa_Acosta.pdf
[32] http://www.nbnco.com.au/assets/media-releases/2011/remote-australians-the-priority-for-new-nbn-interim-satellite-service-06-may-11.pdf
[33] NBNCo Corporate Plan 2012-15: http://www.nbnco.com.au/assets/documents/nbn-co-corporate-plan-6-aug-2012.pdf, page 56

[35] NBNCo Corporate Plan 2012-15: http://www.nbnco.com.au/assets/documents/nbn-co-corporate-plan-6-aug-2012.pdf, page 56
[36] http://www.nbnco.com.au/assets/documents/fixed-wireless-factsheet.pdf
[37] http://www.nbnco.com.au/assets/media-releases/2011/remote-australians-the-priority-for-new-nbn-interim-satellite-service-06-may-11.pdf
[38] ACMA media release 81/2012 – 29 October: http://acma.gov.au/WEB/STANDARD/pc=PC_600087
[39] FCC White Paper " *The Public Safety Nationwide Interoperable Broadband Network: A New Model for Capacity, Performance and Cost"* http://transition.fcc.gov/pshs/docs/releases/DOC-298799A1.pdf
[40] GQ-AAS Report: Public Safety Mobile Broadband Demand Requirements (Project 1) Final Report v2.2 p22 (publicly available version)
[41] http://www.etsi.org/deliver/etsi_tr/136900_136999/136902/09.03.01_60/tr_136902v090301p.pdf
[42] http://www.smh.com.au/news/National/Telstra-to-sue-Coonan-over-CDMA-threat/2007/09/11/1189276708898.html
[43] http://www.telstra.com.au/mobile-phones/coverage-networks/our-coverage/mobile-broadband/
[44] http://www.ericsson.com/news/1443016
[45] http://mediacenter.motorolasolutions.com/Press-Releases/Motorola-Solutions-Brings-First-Commercial-Release-of-Standards-based-LTE-Technology-to-Public-Safety-3759.aspx
[46] ACMA media release 81/2012 – 29 October: http://acma.gov.au/WEB/STANDARD/pc=PC_600087
[47] http://www.ericssonw35.com/index.html
[48] http://www.nbnco.com.au/blog/gallery-nbn-fibre-installation.html