

Prioritization and Pre-emption

- *Have 3GPP standards for LTE fully incorporated pre-emption, and has this been taken up by equipment vendors yet? (By pre-emption, we mean the ability to dynamically reduce/drop active communications of lower priority users during emergency incidents so that public safety users can have sufficient capacity over the network).*
- *If not, are there aspects of preferential access that are still being incorporated into the standards? Or are vendors still working to incorporate these into their products?*

The 3GPP standards have not incorporated pre-emption, at least not as the public safety industry has defined it. Public safety often refer to their desired implementation as “ruthless pre-emption”. The 3GPP has been focusing on prioritization rather than pre-emption. Prioritization is a first-in-queue technology that allows certain classes of priority users to be next in queue for network access. To date, there is no concept in 3GPP of reducing or dropping active communications to make room for First Responders or other high priority users. However, there are ways to manipulate LTE networks to make room for higher priority users (the result is still less than “ruthless”). These traffic management schemes that attempt to load balance and make use of throttling techniques to ensure more users can have access. However, these rudimentary approaches often result in users having an overall poorer quality of experience, because full access to the network resources are restricted.

All 3GPP standards (including those in question) are written as guidelines, and do not explain how the implementation should be done. Therefore, all infrastructure vendors interpret and implement the standards differently. Many claim pre-emption capabilities when they actually offer priority access only. There are many versions of priority access available. Some have been implemented by third party companies and others by the infrastructure vendors themselves. Mostly, the implementation of priority access appears an afterthought, without the capability of assigning priority levels to every subscriber or without the ability to make the prioritization dynamic.

Rivada has taken the ideas of prioritization and pre-emption seriously. In fact, we started our business with the goal of solving this problem for public safety. Today, many of Rivada's ideas for priority and pre-emption are being discussed among the public safety community and some are beginning to find their way into the standards. Still, Rivada's approach is unmatched. No other solutions for priority or pre-emption have emerged that include the breadth of options in Rivada's proprietary technology.

- *To provide preferential access to public safety users, what changes would be required in existing commercial mobile networks (e.g. hardware and software)? Can you give us an indication of the approximate costs involved, and the challenges/complexities?*

Please note that we assume that the question is referring to preferential access for public safety users *on the public safety network*. We also assume that Rivada's Dynamic Spectrum Arbitrage technology is deployed, allowing commercial subscribers to use the public safety Radio Access Network.

Any deployment of Rivada DSA technology inherently provides preferential access to public safety users. The preferential access capability is built-in. Rivada provides equipment to both the commercial mobile operator as well as the public safety operator. This equipment communicates with the respective LTE network components to facilitate the movement of subscribers between networks. Our equipment also provides a mechanism for the buyers and sellers of wireless capacity to conduct their buy/sell transactions. In the context of this question, the public safety operator is the seller and the commercial mobile operator is the buyer. However, either operator could be the buyer and/or seller via a configuration setting.

For early adopters, Rivada plans to cover all of the cost of ownership expenses of implementing Rivada's technology. This means no additional expense is incurred to acquire and configure the network beyond the normal cost of buying and deploying LTE infrastructure.

We expect a low complexity implementation. Our technology makes use of existing 3GPP procedures and the interfaces with LTE network components are implemented between Rivada and the infrastructure vendors without operator involvement.

- *As far as you are aware, have any commercial networks implemented preferential access features to date?*

Many commercial networks have implemented some form of preferential access features. Rivada is unaware of any that have addressed the ideas of priority and pre-emption to the extent that Rivada has.

- *Does the Rivada Dynamic Spectrum Arbitrage (DSA) technology include a user interface that allows Public Safety organisations to control Access to both public safety and commercial networks? Can this User interface be distributed amongst national, regional and local incident centres? What does Rivada consider to be the main challenges to implementing such an approach?*

Please note that this answer first clarifies the meaning of “user interface”, since this term could refer to the screen of a computer terminal or a mobile device:

When using Rivada DSA there is no subscriber involvement with the user interface (screen) of mobile devices. Rivada's DSA technology requires no software changes to mobile devices. The visiting mobile subscriber has no indication that they are roaming on another network; the subscriber needs to take no action to roam. The user experience is seamless while moving within and between networks. The same is true for the mobile device while on the subscriber's home network.

We now discuss Rivada's administrative user interface console housed in a public safety facility, such as a network operations center (NOC).

Rivada provides an administrative interface console that controls the rules/policies under which network capacity is made available for sale and how visiting subscribers are managed during pre-emption. The interface includes analytical tools to help buyers decide which bandwidth to purchase and when. The Public Safety operator controls access to his own network. The access to the commercial network would be controlled by the commercial operator. Note that the terms of the network access will be articulated in a contractual agreement between the operators – the terms include public safety's permission to pre-empt.

Rivada understands that buyers and sellers of network capacity need to have some degree of local influence, especially during times of emergency. Therefore, Rivada is making a system available that can be authenticated for specific geographic sub-regions, under which local control can be exercised. The buyers and sellers of bandwidth could choose how they would like to partition decision making authority, by administrative privilege level at the NOC console and/or by geographical area.

Roaming

- *If public safety users were to be given the ability to roam from a dedicated network on to existing commercial networks (e.g. to boost coverage or capacity), what technical changes would be required on each network (e.g. hardware/software)? What are the associated challenges, complexities and costs?*

In any deployment of Rivada DSA technology, we provide equipment to both the commercial mobile operator as well as to the public safety operator. No other hardware or software is required. Furthermore, no changes are required on the mobile devices themselves.

Any deployment of Rivada DSA technology inherently provides the ability for commercial subscribers to roam onto the public safety network and/or public safety subscribers to roam onto commercial networks. Our equipment allows either (or both) networks to become sellers/buyers of wireless capacity.

Like any other carrier grade infrastructure, there will be some nominal cost of ownership. It is likely that third party companies will provide services related to installing, configuring, managing, and maintaining the Rivada hardware nodes and software. Established network infrastructure vendors may someday offer Rivada DSA technology as an option for those who want to buy and sell capacity. We expect that new companies will be established around the burgeoning industry to help network operators manage bandwidth marketplace technologies. For early adopters, Rivada plans to cover all of the cost of ownership expense of implementing Rivada's technology.

Network cores

- *To what extent would the lower volume of traffic and users over a public safety network (relative to a commercial mobile network) reduce the cost of a network core? What would be the approximate cost of a commercial and a public safety LTE core?*

Assumption: This answer assumes that Rivada Dynamic Spectrum Arbitrage technology is deployed on the public safety and commercial networks in question.

Normally the mobile operator that is selling capacity to roamers needs to dimension their radio access and core networks to handle all roaming traffic as though it was their own. Rivada's DSA technology relieves a great deal of this burden from the bandwidth provider's network. We do this by employing techniques such as home-routed traffic. The result is that the traffic from the visiting subscribers is carried on their home core network. Another essential benefit gained is that the visiting subscriber's session continuity is maintained when moving between networks, leading to a seamless and high quality of experience.

The net result of a Rivada-DSA enabled public safety network is that the core network capacity requirements are somewhere between a pure public safety network and an outright commercial network, but leaning closer to the size of a typical commercial network. The dimensioning will therefore be very dependent on the projected volume of commercial traffic.

Separately, we consider the case of a Mobile Virtual Network Operator (MVNO). These operators, such as Virgin Mobile, do not have their own network. The MVNO's subscribers use the network of other Mobile Network Operators (MNOs). In the case where the public safety network is hosting MVNO subscribers, the public safety network must carry the core network traffic of the visiting subscribers. This means that the required capacity of the core network for serving the MVNO subscribers will be similar to that of an MNO.

Deployables

- *Are you able to provide any information on the technical specifications of the deployables/transportables that could be used to meet public safety needs? What are the approximate costs associated with purchasing and operating these (e.g, cost of having them on standby then mobilising)?*

Deployable infrastructure comes in many configurations and can be largely dependent on the backhaul mechanism used. These deployables can be designed to function as part of an LTE network for network capacity augmentation or as an independent stand-alone network for remote rescue missions, bushfires, marine use, etc.

For the capacity augmentation scenario, sites are typically on trailers with short crank-up towers. The more compact versions for stand-alone deployment should be ready to be air-dropped or carried, mounted to vehicles, or carried by truck into disaster areas. Today, it is most common to see trailer mounted electronics, equipped with a portable generator and auto deployable satellite backhaul.

The following are some typical quantities deployed: Clusters of approximately 5 trailer or vehicular mounted base stations should be staged both in major cities and centralized in remote areas for air drop deployment. Any regularly patrolled area subject to ongoing police action will normally have a few vehicles outfitted with transportable base station electronics. The rule of thumb is that outlying areas should have access to deployables within 3.5 hours by vehicle or air drop.

Costs vary widely depending on the strategy for mobilizing deployables. Rivada currently sees that most major cities have a few deployable base stations on hand while there are typically a few dozen available for remote national deployment from central locations. Exact numbers of deployables and warehouse locations will depend on size of the country, proximity of remote areas to large urban centers, distance to farthest extent of deployment areas, historical volume

and size of incidents, etc. Remote warehouse locations are typically near Army Reserve, Military Bases, Emergency Response Centers, etc., where facilities/airports and personnel already exist that can rapidly deploy infrastructure. Operational experts needed to setup and configure electronics are often flown in from other locations (urban centers) and can arrive after transportable infrastructure arrives and is physically assembled/ready for use. There are seldom dedicated electronics experts living at the same location where the infrastructure is warehoused (only transportation and/or assembly experts are within proximity of the warehouse). This reduces costs, since resources can be shared with other emergency response and military organizations who already have functioning warehouses, operation centers and transportation equipment that can be operate under a shared budget. Equipment can also be deployed by contractors who are similarly positioned.

Rivada recommends budgeting an average of \$350,000 AUD per deployable with a range of \$250k-\$600k AUD.

- *Is there any technical/cost information on in-vehicle deployables that you can provide (e.g. where the deployable arrives on scene with the incident commander)? What technology would these use for backhaul and local access?*

Backhaul is the Achilles' heel of deployable wireless infrastructure. Traditionally satellite has always served as a reliable means of interconnect for deployable infrastructure. However, the case for satellite backhaul is much less compelling due to slow backhaul speeds and high cost of satellite equipment that is easy to configure.

In urban areas there are many more backhaul options that are quicker to configure and capable of much higher speeds. These mainly non-line-of-sight technologies, including vehicular modems, can use commercial cellular bandwidth (if available) or possibly self-configuring microwave. However these systems often leverage unlicensed spectrum and are considered less reliable in times of emergency. The bottom line is that there is no easy backhaul solution to deployables (in-vehicle or otherwise).

One use case for in-vehicle deployables assumes the use of swarm technology, where every mobile device communicates through other mobile devices or communicates locally through a local wireless network with no dependency on long-haul transport. These systems are easier to deploy and much less expensive, however they only work effectively when the bulk of the communication needs to happen between First Responders all located within the immediate area of an incident.

Rivada recommends budgeting an average of \$125,000 AUD per in-vehicle deployable with a range of \$60k-\$180k AUD.