



A comparison of communications Network Architectures for a Public Safety Mobile Broadband Network

700 MHz Mobile Broadband for Public Safety - Technology Advisory Group

Public Security Science and Technology

October 7, 2011

Partners: The Technology Advisory Group for 700 MHz Public Safety Spectrum (700TAG) is composed of a collaborative group of technical experts led by Centre for Security Science and includes scientific authorities from the Communications Research Center, and technical experts from Federal/Provincial/Territorial/-Municipal agencies.

Objectives

The objective of this Technical Advisory Note (TAN) is to inform the Canadian public safety community on the advantages and disadvantages of two forms of communications network architectures that can apply to a Public Safety Mobile Broadband Network. The implications for governance and operations associated with each option are also discussed.

Communications Network Architectures for Public Safety

The two network architectures that are reviewed in this TAN are,

- One national network, and
- Federated regional networks

As far the Users are concerned, the matter of which architecture is adopted is irrelevant as long as they are able to use the services delivered across the network to conduct their missions efficiently. Either one will deliver the services transparently to the User and can be implemented within a Public Private Partnership (PPP) model. The choice of network architecture has a bigger impact on governance, operations, and maintenance than on the usability. All levels of emergency management, from municipal to federal, are involved to different degrees for one model versus the other.

A conceptual-level comparison of two communications network architectures is presented. The dimensions which are covered in this TAN are intended to illustrate fundamental differences between the two approaches from the perspective of operability and interoperability for public safety purposes. It is not intended to be an

exhaustive comparison of the network architectures.

One National Network

Figure 1 illustrates what a national network could look like. All regions are interconnected at a central location. Redundant connections and facilities are not shown in order to simplify the illustration. This architecture is similar to an enterprise network where regional centres would establish encrypted Virtual Private Network (VPN) tunnels over the public Internet to access their services from the central host. The central host would provide access to the Internet and interconnection to other carriers.

Roaming agreements with commercial carriers would be negotiated at the national level. The Network Operations Centre (NOC) would monitor the performance of the operations across all regions and initiate corrective actions as required. Regional Op Centres would address local User issues. The need to monitor the performance of the services delivered to public safety users would be required whether the infrastructure is shared with a private partner or not.

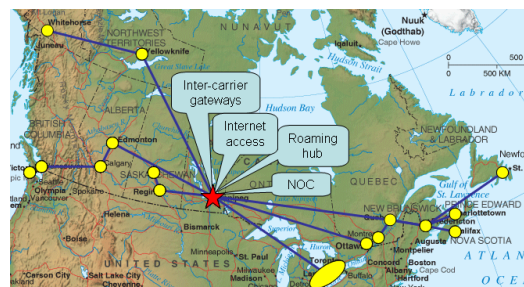


Figure 1: Illustration of one national network architecture.

Application servers would be located according to the type of information they contain and their purpose. For example, servers containing national crime information data would be located at the national level. Whereas, servers that contain building plans and hazmat inventory would be



located at the regional level. The distribution of data repositories would not be affected by the choice of network architecture and redundant locations would be implemented as backup in case of failures.

One of the advantages of having a single national network is that it is less costly to operate since it avoids the duplication of resources and back-office infrastructure at all the regions. Another advantage is the simplicity of administering roaming permissions. Being a single network, all registered users are considered to be in their home network no matter where they are.

A major drawback of this network architecture is that the regions require a robust connection to the central core network. If a connection to one of the regions were to fail, it would not be acceptable for the service to that region to also fail. In order to increase the resiliency of the network, each region would need to replicate many of the functions of the central core. That means that the regions would also need to have qualified staff, operational procedures, and an administrative structure to be able to operate autonomously in case the connection fails. Then, the cost of one national network would no longer be an advantage when one considers the additional cost to harden the connections and the replicated operational infrastructure in each region.

Federated Regional Networks

The concept of federated regional networks is based on the network-of-networks with emphasis on the cooperative aspect of the federated nature of the networks. A region may be a province or a collection of provinces or a large metropolitan area. Figure 2 illustrates the concept of federated regional networks. Note that most capabilities are de-centralized towards the regions. However, the Roaming Hub remains at the national level. This facilitates the seamless movement among Users across all the regions and of roaming onto commercial networks. It also simplifies the roaming of US public safety personnel, when authorized, on any of the regional networks. To all other carriers, the federated regional networks would appear as one network with one internationally recognized Public Land Mobile Network Identifier (PLMN ID).

Each region would access a nationally-hosted database of Users through their regional portals in order to register the Users and their associated

profiles. Federal agencies could register their Users at the national or regional levels. The database would be replicated in all the other regions so that Users transiting between regions could do so without being re-authenticated. They would have access to local and national services as well as their home-based services.

The interconnection to commercial carriers would be at the regional level, even though the Home Subscriber Server (HSS) is at the national level. Each region would have its own NOC. Because the connection to the Internet would be at the regional level, a regional network operator can set and assert its policies with regards to Internet access controls, which may be different from those of another region.

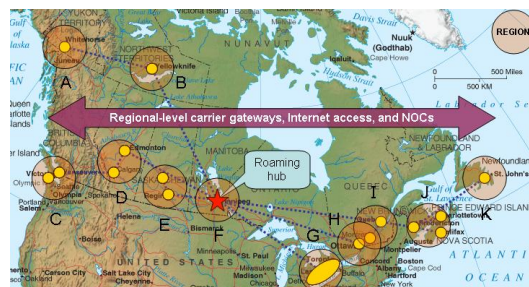


Figure 2: Illustration of Federated Regional Networks architecture.

The major advantage of the architecture based on Federated Regional Networks is the resilience of the network. Each network can operate independently of the national core network, but roaming may be adversely affected if the connection fails. The traffic flowing between the regions and the national core is minimal, consisting mainly of management and control information and that which resides on national servers. With local caching of national databases the information flow can be reduced even further. This could be particularly important for those regions that may have unreliable connectivity to a national core.

A major disadvantage of Federated Regional Networks is the elevated risk of non-interoperability because the regions may choose to implement their networks with different partners. In order to mitigate this risk, the regional network operators and the national-level operator could agree to adopt a minimum set of interoperability requirements. The second level





risk associated to this is the potential for networks to become non-interoperable over time if each region and its partner upgrades the network at different times and in different ways. To mitigate this risk requires a deeper level of coordination and cooperation among the regional and national network operators and their partners. Another action that should be taken is to validate the interoperability of new features and upgrades in a system-level test facility to identify potential issues before they are implemented on the live networks. Such a test facility could be implemented at the national level to serve all the regions.

Network expansion

A further consideration in the selection of network architecture is how the expansion of coverage and/or capacity can be done. It is highly likely that the expansion of the network will occur over a period of time as capital budgets would allow. Expansion for coverage or for capacity takes the form of adding new infrastructure, which could include additional backhaul capacity for those connections where the capacity is inadequate to support the additional data and control traffic. LTE accommodates the addition of new infrastructure inherently at the edge of network. This means that there is little, if any involvement of the core network to turn up the additional infrastructure. There is, however, some operational and administrative involvement to manage the unique identifiers of the infrastructure. This is not deemed to be a significant burden for either network architecture.

Comparison and Summary

Table 1 summarizes the relative advantages and disadvantages of the One National Network architecture and the Federated Regional Networks architecture for different attributes. The  symbol indicates an advantage of one network architecture relative to the other. Conversely, the  symbol indicates a disadvantage of one versus the other.





















Attributes	One National Network	Federated Regional Networks
Administration of roaming agreements		
Administration of upgrades		
Administration of user profiles		
Performance of applications		
Cost of infrastructure and operations (national and regionally)		
Ease of governance for interoperability		
Inter-jurisdictional roaming		
Regional jurisdictional autonomy		
Network resilience and reliability		
Network expansion		

Table 1: Comparison of One National Network versus Federated Regional Networks.

Conclusion

Two network architectures were evaluated from high-level perspectives of interoperability, governance, operations, and maintenance. With respect to the attributes used in comparing the two network architectures, neither one appears to have a strong overall advantage over the other one. However, if one applies different weights to the attributes then a favoured architecture could surface. For example, if ease of administration for interoperability is most important, then the One National Network model is more suitable. On the other hand, if regional jurisdictional autonomy and network resilience carry higher weight, then the Federated Regional Networks architecture is favoured. This is not to suggest that interoperability could not be achieved with Federated Regional Networks, or that One National Network cannot be made to be resilient. A weighted comparison highlights what architecture is more amenable to different attributes.



More detailed information and other perspectives on one national network vs. network-of-networks can be found in the documents referenced below.

1. NPSTC position paper, "The Need for a Nationwide Broadband Concept for Public Safety", March 10, 2011
<http://www.npstc.org/download.jsp?tableId=37&column=217&id=1047&file=NPSTC%20Position%20BB%20Network%2020110310.pdf>
2. FCC Emergency Response Interoperability Center, "Nationwide Interoperability Framework", presented at Public Safety Communications Research, Boulder, CO, Dec. 2, 2010.
http://www.pscr.gov/projects/broadband/700mhz_demo_net/stakeholder_mtg_122010/day_2/4_nationwide_interoperability_framework_fcc.pdf

NOTE: DRDC Centre for Security Science warrants that this advisory note was prepared in a professional manner conforming to generally accepted practices for scientific research and analysis. This advisory note provides technical advice and therefore is not a statement of endorsement of Defence Research Development Canada, Department of National Defence, or the Government of Canada

Author: Claudio Lucente, P.Eng.

Scientific Authorities/Approval for Release: C. Belisle, J. Pagotto