NPSTC Broadband Task Force
Governance Group

Roaming and the Shared Wireless Broadband Network

11 August 2009 - V4

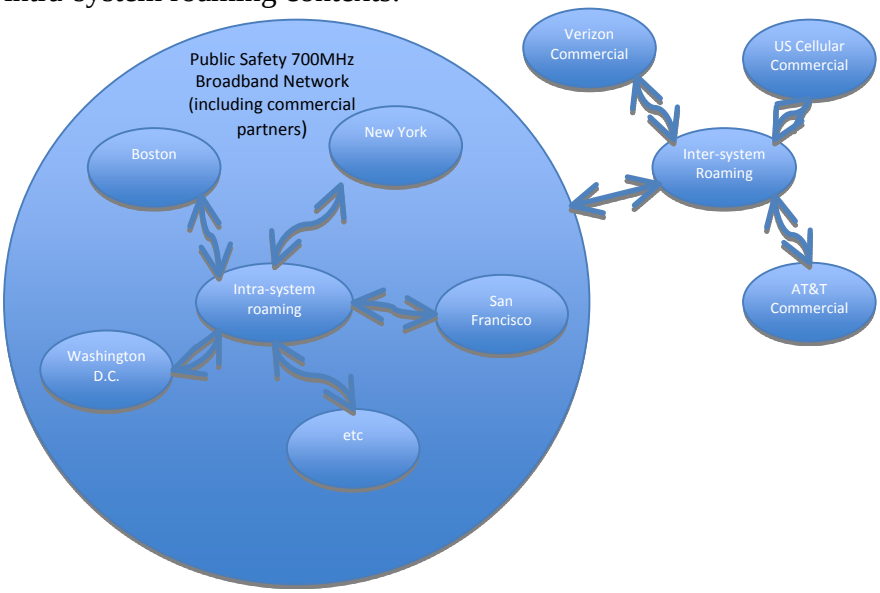
Introduction

In exclusively commercial mobile networks, roaming is an essential capability for providing users with the experience of national connectivity. Even after twenty-five years of development and tens of billions of dollars of investment, no single terrestrial mobile service provider in the United States can provide a truly national footprint to its customers without relying on roaming services from other operators. A nationwide, interoperable wireless broadband network, referred to here as the National Broadband Data System (NBDS) for public safety will not be built overnight and it will take many years to even approximate ubiquitous coverage. During that period, the ability of public safety users to roam on commercial networks will be essential. Likewise, while not a first order priority for public safety, the ability of commercial users to roam onto the NBDS, utilizing otherwise idle capacity may be essential to rendering the NBDS financially viable in much of the country.

Roaming between the NBDS and commercial networks will be referred to in this paper as "inter-system" roaming. Inter-system roaming requires interworking at the business and operational levels including not only network authentication, but also bilateral roaming agreements between the Public Safety Broadband Licensee (PSBL) and commercial networks in addition to some type of clearinghouse mechanism to settle accounts between parties.

This paper will also address "intra-system" roaming. The vision is that the NBDS will function, to the extent possible, as a single network. Significant elements of that network may be shared. It is also possible that elements of the network may be owned and operated locally, either by "local builder" public safety agencies or by D Block licensees or other private commercial partners. Depending on which elements are deployed and managed locally and which are shared across the NBDS, "roaming" arrangements may be required between participants in the NBDS. In the world of circuit-switched mobile voice services, for example, this type of roaming occurs *within* the networks of every multi-regional service provider since platforms for user authentication such as Home Location Registers (HLRs) and Visiting Location Registers (VLRs) are associated with each Mobile Switching Center (MSC) in an operator's network. The architecture of mobile data networks is not as geographically-constrained, so the deployment strategy for analogous elements, such as Packet Data Serving Nodes (PDSNs), Gateway/Serving GPRS Packet Support Nodes (GGSN/SGSNs) is more a matter of network reliability, economic efficiency and governance considerations than a fixed technical requirement.

The following diagram illustrates possible relationships between parties in the inter- and intra-system roaming contexts:



Roaming Categories

The Broadband Task Force Technical Working Group has identified the following requirements for roaming:

- In the absence of coverage from the home network, the ability for the User Equipment (UE) to scan supported bands, perform cell selection and authentication on a visited network
- After authentication on a visited network, the assignment of an IP address, and the ability to communicate with the public Internet
- Handoff of active sessions / calls between home and visited networks is required when both networks are using LTE technology
- Handoff of active sessions / calls between home and visited networks is not required when a visited network is using earlier generation wireless technologies.

Authentication: The primary function required to support roaming at the network level is authentication. In order to operate a device on a mobile network, user equipment must be authorized for use on that network. This is a function performed in every mobile network regardless of whether a customer is roaming or operating within the home network. As noted above, in circuit-switched (non-IP) voice networks, the distinction of "home" and "visited" network is an important one. Networks are defined around individual MSCs and, even when using their own service provider's network, users are roaming whenever they attempt to operate a mobile device outside their home area. For data services, these boundaries are not as important from a technical architecture standpoint. Assuming that the NBDS is functionally a single network, local components of that network would likely share national platforms for authentication and that sharing would likely be governed by Network Sharing Agreements (NSAs) between those local participants (local builder public safety agencies and/or commercial D Block licensees) and the

PSBL. If necessary, authentication could be provisioned on a local or regional basis, in which case local areas would function, from an operational standpoint, more as individual networks. This decision is driven to a greater degree by governance and operational control considerations than by the technology.

Delivering this operational capability, however, requires more than performing the required functions in the network. Roaming, particularly "inter-system roaming" as we have defined it here, requires business arrangements between network operators. This aspect of roaming, which encompasses the commercial and legal frameworks between network operators, consists of two primary elements:

Roaming Agreements: Intra-system roaming can be governed by NSAs and is primarily a function of validating and authorizing users. Roaming between systems, on the other hand, usually involves additional, more formal, arrangements. Commercial carriers exchanging roaming traffic typically execute bi-lateral roaming agreements. These agreements identify geographic areas, define rates and other commercial terms, and specify certain technical requirements. Agreements to facilitate roaming between the NBDS and commercial networks could follow either of the following models, depending on a variety of factors, including whether the D Block is included, and if it is included, how it is ultimately licensed:

1. Agreements between the PSBL and commercial roaming partners – the preferred model if the entire NBDS is operated by public safety rather than under NSAs with D Block licensees.
2. Agreements between the local/regional operators of "sub-networks" (either public safety "local builders" or D-block licensees)

Roaming Settlements: Roaming traffic is not always symmetrical between networks and, in the commercial context, it is generally necessary for roaming partners to settle net differences through some clearing mechanism. This is one role that companies like Syniverse and TNS play in the roaming process. If, within the NBDS, owners and operators of parts of the network are willing to allow roaming without this type of settlement, the process can be simplified. However, to the extent that significant asymmetries produce a financial burden on some operators or parts of the network, this mechanism may be important even in the "intra-system" context. If a financial settlement is required between entities that are part of the NBDS, it could be managed by the PSBL (perhaps outsourced to a clearinghouse) rather than by individual arrangements between local entities. It is worth noting, however, when considering these asymmetries, that one important roaming scenario involves mutual aid situations. In these contexts, the beneficiary of the roaming activity is really the region receiving the roaming traffic and it may be inappropriate for a region experiencing a major incident to charge roaming fees to agencies coming to its aid.

The following table lays out the difference between inter and intra-system roaming as it relates to the three functions discussed above.

	Inter-Network Authentication	Roaming Agreement	Clearinghouse/Settlements
Intra-System Roaming PS user roaming onto another part of the NBDS outside the home area.	Depends on the architecture. Yes, if each local area operating its own PDSN. No if that function is shared.	Perhaps not, provided that agreements with the PSBL allow the PSBL to facilitate any required flow of funds between owners/operators of local components of the NBDS.	Yes, if a flow of funds is required between owners/operators of local NBDS components.
Inter-System Roaming without commercial D Block licensees PS user roaming onto a commercial network or commercial user roaming onto the NBDS.	Yes	Yes. Likely bi-lateral agreements between the PSBL and commercial roaming partners.	Yes.
Inter-System Roaming with commercial D Block licensees PS user roaming onto a commercial network or commercial user roaming onto the NBDS.	Possibly. Inter-network authentication may not be required if roaming onto the commercial network of the D Block licensee serving that PS user's area.	Yes. Likely bi-lateral agreements between the PSBL or the D Block licensee in that area and other commercial roaming partners.	Yes.

Conclusion

Roaming capabilities are essential to providing users of the NBDS with seamless or near-seamless nationwide services. Delivering those capabilities requires functionality in the network to support authentication. It may also require legal and financial arrangements between network operators and between operators and a clearinghouse provider. As with many other issues related to the NBDS, the specific arrangements depend on both technical and governance considerations, including roles played by the PSBL, local builders, and D Block licensees/private commercial partners in building, owning, and operating the network.