Shared Networks -

Performance Management Challenges

Executive Summary

The concept of network or infrastructure sharing is well understood with many different business models to choose from. However, what is not well understood is how to successfully manage a shared network and ensure appropriate visibility to the network operator to achieve revenue growth and to ensure the long-term viability of the network share.

The purpose of this white paper is to examine some of the challenges of managing a shared network, and to give guidance on aspects to consider to ensure visibility for the operator of key business indicators while delegating day to day operations to the joint venture managing organisation.

Background

The mobile landscape has changed dramatically since data rates became fast enough for mass market uptake of data services. The introduction of smartphones and other mobile devices to avail of these data rates is driving a change in consumer behaviour from simple requirements for file download, to fast upload of high levels of photos and data, and requirements for streaming video.

The demand for increased bandwidth, coupled with the flat-fee service charging model for data, and high license and network management costs, have required network operators to seek new ways of reducing both CAPEX and OPEX costs while increasing coverage and meeting capacity demands. Network sharing is increasingly being adopted as an approach to resolving these problems.
Network Sharing

Network sharing is where two or more network operators agree to share resources or infrastructure in order to reduce the costs of building and maintaining a network.

Network sharing can be achieved at different levels which are broadly separated into the following categories as shown in Figure 1:

- Passive Site Sharing with pure site sharing only (possibly including cabinets, power, masts, antennas etc)
- Passive Site Sharing with site and access sharing (where the backhaul is shared but not the radio equipment)
- Active Site Sharing (Multi-Operator Radio Access Network - MORAN) where the BTS/NodeB/eNodeB and possibly the BSC/RNC are shared. Each operator maintains its' own cell level parameters and only site level parameters are shared.
- Active Site Sharing (Multi-Operator Core Network - MOCN) where the BTS/NodeB/eNodeB and BSC/RNC are shared AND the frequencies are pooled. In this case the operator cannot control its network at cell level.
- Roaming Based sharing with shared RAN and Gateway Core where one operator relies wholly on another operator for coverage for a certain, defined footprint on a permanent basis but separate core networks are maintained.
- Roaming Based sharing with full network sharing where the operators separately work as Mobile Virtual Network Operators (MVNOs), holding only home location registers, authentication and billing information systems in their own right and all other aspects are shared.
Each level of network sharing brings savings to the operator but at a cost of reduced control over that aspect of the network. Operators need to consider the most appropriate solution for their market, considering aspects such as cultural alignment with the potential partner, level of coverage and control required, the level of risk acceptable in merging the networks, shareholder and cost pressures etc.

For the purposes of this white paper, the technical solution assumed is that of the MORAN approach where Radio Access Network equipment is shared but frequencies are not.

**MORAN Network Sharing**

In the case of MORAN Network sharing, two or more operators agree not only to share sites, but also to share the BTS/NodeB/eNodeB equipment on the sites. They also share the transmission network and usually share the BSC/RNC equipment which is connected to the respective operators’ core.

---

1 From *Infrastructure Sharing for Mobile Network Operators* Dr. Thomas Frisanco, Member, IEEE, Dr. Paul Tafertshofer, Pierre Lurin Nokia Siemens Networks Munich, Germany
networks (See Figure 1). Separation of the operators’ networks is managed by the use of dedicated frequencies as awarded by the licensing bodies, on which they can broadcast their own individual network identifiers. The advantage of the use of a MORAN network sharing approach is that there are significant CAPEX and OPEX savings as the numbers of both site and equipment can be reduced. Disadvantages of this network sharing approach include:

- Difficulty in creating competitor advantage as they will be operating with the same equipment vendor, software version, optional features, and with similar coverage and quality.
- New service introduction (that require new software or hardware) may require joint agreement, curtailing the ability of one operator to achieve first mover advantage.
- Network sharing will largely force alignment on technology evolution.

As network sharing requires a high level of operational management, this is generally best handled as a joint venture which acts as a service provider managing the network planning, operations and maintenance functions on behalf of the sharing operators. This is increasingly achieved through the outsourcing of the joint network operations to a managed services vendor.

Figure 2: Typical Management Structure of MORAN Network Share
The management model thus looks as is in Figure 2, with the Joint Venture Managing Organisation (JVMO) managing operations and the alignment of technology, and the operators focussing on Business Support Level (Billing, customer care etc.) for differentiation of their offerings to their customers.

Management of a MORAN Network Share

Fault and performance metrics supplied by the access network are key to understanding how the network is performing (the accessibility, retainability, integrity, mobility, utilization and availability of the network). These metrics are the building blocks to inform strategy and planning, and also to minimise churn and ensure good customer relations management.

When managing these metrics in a shared network environment, the following needs to be considered:

- Data Governance – High level policies and agreements around the ownership, access and security of specific data
- Data Management – The approach to collection and storage of the data
- Data Integrity — The accuracy and completeness of the data.
- Data Content – The type, frequency, granularity of data required

Data Governance

In the traditional industry structure, all fault and performance data belonged to the one operator. With the introduction of network sharing, it has to be decided which information belongs solely to a particular operator, and which information must be shared. For example, whereas it is easy to distinguish ownership of data at cell level, there may be some capacity related or backhaul related information that may need to be shared between the operators in order to make strategic decisions on capacity enhancement.

A mobile network has the potential to deliver a huge volume of fault and performance metrics, so high level policies need to be agreed in terms of
operator requests for activation of metrics (volume of metrics to be activated, number of requests per day/week etc.) as these requests require resources to fulfil, processing capacity on the network and OSS servers for collection and storage.

With the network share, security becomes very important, as any breaches in security, whether intentional or not, could allow the data to be accessible by a competitor operator.

Another aspect that needs to be considered is how to manage the collection and handover of data in relation to Legal Intercept, where call data records sit with the operator but network related and location data sit in the JVMO.

**Data Management**

Once high level policies are agreed between the operators and the network management entity, then a collection and storage solution needs to be determined.

The following are typical questions that need to be resolved:

- Is the operator willing to duplicate or host any part of an OSS solution (such as a complex database and post-processor).
- How is the data transferred from the network management entity into the operator domain, what type of data encryption will be used.
- Will the operator need to introduce new databases to store the data, or will it have direct access to databases in the network management entity.
- How is filtering achieved to separate out information belonging to the different operators. How is shared data accessed and managed.
- How are the operator post-processing tools updated to deal with filtered data.
- How are data structure and format changes (due to network or OSS software updates) communicated to ensure post-processing tools are prepared for such changes.
• How often will data be transferred to the operator network, in near-real time, hourly, daily etc.

**Data Integrity**

Within an organization, acceptable data quality is crucial to the reliability of business analytics (BA) / business intelligence (BI) reporting. Aspects of data quality include accuracy, completeness, relevance, consistency across data sources and accessibility. Data quality is affected by the way data is entered, stored and managed.

The operator may need to introduce some independent method to audit the data to ensure data quality is acceptable. This method may include correlation with independent drive testing, probe or core network metrics.

**Data Content**

With the introduction of a network share, many network related responsibilities move towards the network managing organisation; however BSS responsibility remains within the remit of the operator including Product Management, Order Management, Customer Management, Revenue and Fraud Management, each requiring a different view of the underlying access network (Figure 3).
Executive

At executive level, a set of auditable SLA metrics should be agreed between the operator and the network management entity. These may include metrics such as:

- Reaction and resolution times for outages and degradations
- Build rates for new sites
- Rate and quality of resolution of incident and change requests
- Repeat fault rate

Planning / Strategy

As discussed earlier, with the introduction of a MORAN network share, strategic technology alignment must occur. However, on an individual operator level, planning and strategy must have the necessary fault and performance metrics to plan appropriate services, coverage and capacity. These metrics may need to be at a very detailed level, as statistics may
need to be able to differentiate phone types, services (e.g. streaming, interactive, voice), APN usage, application usage, handover rates (e.g. to WiFi, 2G etc.) down to cell / cluster level.

**Product Management / Sales and Marketing**

Product management and sales and marketing need to work closely with the planning and strategy departments, using similar metrics to determine the best product offerings that fit with the coverage and capacity offered by the network.

**QoE / Customer Management**

Quality of Experience (QoE) is a subjective measure of a customer's experiences with a service and has become a key factor in reducing churn. Traditionally, assurance comprised solely of resource assurance, i.e. managing the capacity, uptime etc. of the nodes in question. With the convergence of networks and services and the multiplication of products, the concept of Service Fault and Quality Management emerged, relating network end-to-end performance to business objectives. However understanding how services perform is no longer enough. Customer-centric monitoring of multiple aspects of the total customer engagement is required.

In order to measure QoE effectively, handset data (e.g. phone type, screen type, wireless capabilities), data on phone behaviour in the network (handovers, signal strength, call attempts etc.), core network probe information (APNs used, different QoS services used), charging information (Radius), incident related information (e.g. outages or poor coverage in areas in which the phone was moving) need to be correlated to achieve the full picture.
Customer Care

Customer Care needs to be able to correlate customer complaints against fault and performance information from the network, to ensure appropriate feedback to customers. This requires near real-time fault, impact and resolution plans to be available.

Other Management Issues in a Network Share

Interoperability with Femto-cells/H-eNodeBs

Femto-cells are small low-power base stations typically designed for use at home or in a small business to improve coverage and capacity (and in some cases to off-load data from busy macro-cells). The femto-cell is connected to the operator network via a broadband connection. It is assumed that because femto-cells (and H-eNodeBs in LTE) are generally deployed to a specific customer on a particular frequency, these cells will remain in the ownership of the operator\(^2\).

The advantage of the femto-cell remaining with the operator is that the operator has the customer relationship and is responsible for the backhaul.

However, this means that it is more difficult to include the effects of the femto-cell in the macro-network radio and handover planning, as the JVMO has little influence over the operator defined power / frequency / scrambling codes used by the femto-cell to minimise interference.

In order to mitigate this, there are two possible approaches:

- The JVMO manages the radio planning aspects of femto-cells with strict SLAs agreed to ensure the macro-cell quality is not enhanced to the cost of the femto-cell quality.

\(^2\) Femto-cells are now also being deployed in public and rural areas with open networks [http://www.smallcellforum.org/Files/File/SCF-Small_Cells_White_Paper.pdf](http://www.smallcellforum.org/Files/File/SCF-Small_Cells_White_Paper.pdf)
The operator continues to plan the femto-cells to agreed SLA levels that do not degrade the quality of the macro-cell.

Both of these approaches require definition of clear quality and interference levels that are reasonable to expect, and methods to monitor and report behaviour in near-real time to the other organisation.

**Inter-operability with Wi-Fi and other technologies**

As discussed in DANU Technologies’ white paper Mobile Data Traffic & WiFi Offloading – Briefing Paper, many operators are introducing a mobile data offloading strategy due to mobile technology (2G, 3G) having limited resources for carrying the large volumes of data traffic. Wi-Fi, femto-cells (as discussed earlier) and WiMax are three different technologies available for data offload. In this paper we focus on Wi-Fi, as it is more widely used today than WiMax, and is available as standard in most smartphones and devices.

Wi-Fi allows a device to connect to a wireless access point connected to the broadband network. Wi-Fi typically gives a higher bandwidth than mobile technology and uses unlicensed spectrum (thus causing little or no interference with the mobile technology). Many smartphones and devices are designed to ‘look for’ Wi-Fi networks (i.e. to monitor the signal strength of Wi-Fi networks) and move to these if the signal quality is sufficient.

In relation to shared networks, the operator will need to measure the impact on traffic as Wi-Fi hotspots are rolled out and co-ordinate with the JVMO to ensure aligned traffic management.

---

3 Note that WiFi is only used presently for data traffic, voice traffic remains on the circuit switched mobile network.
Location Based Services

Over the top services offered by the operator may require location information. This location information now sits in the joint venture management organisation rather than the operator organisation. Increasingly however, applications on smartphones are gaining the location directly from the handset, rather than through network information.

Summary

Network sharing has huge potential for CAPEX and OPEX savings for operators. But these advantages can only be achieved with serious consideration of the practicalities of managing a network share, including the governance and management of the necessary data for running the network. This management is further complicated by the use of data offload techniques such as femto-cells and Wi-Fi, the effect of which must also be considered by the operator.

DANU supports network operators and vendors to implement shared network operations, focusing on the OSS domain, including Service Assurance and Performance Management. We provide consultancy, software and systems integration, drawing heavily upon our investment in research and innovation to deliver technology-enabled business processes.