White paper

Reliable and Scalable TETRA networks

Abstract

The evolution of TETRA networks towards an all-IP architecture is now a reality and has been accepted by even the most demanding users of TETRA technology. Although circuit switch based TETRA networks are still operational and are even still being rolled out today, the trend is towards deploying open IP-based solutions for both small and large TETRA networks. In this context, an all-IP architecture means that both the core of the network and the transport network are based on open IP standards and solutions.

Users who are considering investing in an all-IP architecture for their TETRA networks have a number of options available to ensure mission-critical reliability and scalability. In the past, proprietary IP protocols and equipment were developed by TETRA network suppliers to cope with the limited redundancy features and performance of standards-based Commercial Off The Shelf (COTS) routers, switches and link equipment, resulting in scalable but proprietary solutions. Other TETRA network suppliers did recognize the benefits of using low-cost standards-based IP equipment, but did not really care about reliability and scalability.

With the recent arrival of carrier-grade IP networks based on Multi Protocol Label Switching (MPLS), it is now possible to benefit from standards-based IP equipment when building large TETRA networks with excellent reliability, scalability and performance for mission-critical applications.

This white paper considers the reliability and scalability aspects of the different TETRA network architectures, and investigates whether modern IP / MPLS networks can be of benefit to each of the known TETRA network architectures.

The evolution of IP

Early data communication in the 1960s was based on dedicated links using modulation in the analogue domain. In order to support dial-in over telephony networks, modems were developed during the 70s and 80s that could connect to standard 2-wire Plain Old Telephone Systems (POTS) lines with speeds of 300 to 1200 bit/s. By using adaptive modulation and echo cancelling techniques, modem manufacturers were able to speed this up to 56 kbit/s.

The introduction of Integrated Services Digital Network (ISDN) allowed for a moderate increase of data throughput to 64 or 128 kbit/s. Although still circuit-switched and with a relatively low throughput, the speed of dialling and the reliability of ISDN made it very popular for dialling to Internet Service Provider (ISP) networks.

In the 1980s, the telecom industry started developing packet-data standards and solutions for reliable and flexible transport of data for a wide variety of government and enterprise applications. A good example of such a standard is X.25, which is still widely used, for instance by Automatic Teller Machines. The reliability of this type of telecom equipment is good, but the cost of equipment is high and performance is very limited with a typical speed of 64 kbit/s.

Frame relay (FR) was the next step in the evolution towards native IP for Wide Area Networking (WAN). The frame relay protocol is designed to interwork with ISDN protocols and is mostly deployed over E1 or T1 links, offering virtual circuits with a typical throughput of up to 2 Mbit/s. Its simplicity and ease of configuration made frame relay equipment very popular, but due to the limited bandwidth and routing performance, the technology has become obsolete.

Asynchronous Transfer Mode (ATM) resolved the issue of the limited bandwidth and routing performance of frame relay, offering a throughput of 155 to 622 Mbit/s, based on fibre optic technology.

Although originally developed for voice and data, ATM is mostly used today as a transport layer in ADSL last mile connections and UMTS backhaul networks. Despite its high reliability and high throughput, ATM is considered too complex and costly for future IP network deployments, and it is quickly becoming obsolete for telco backhaul applications with the introduction of Fibre To The Home (FTTH).

The final step in the evolution towards all-IP is the introduction of native IP on top of fibre optic, copper or microwave links. This means that synchronous links (TDM, ATM, FR) are no longer needed to carry IP packets. Instead, the IP packets are carried asynchronously over the link, similar to Ethernet. This results in higher capacity of links due to lower protocol overhead, more bandwidth flexibility, and simpler (thus less costly) and more reliable equipment.

Reliability aspects

When it comes to reliability, the interconnection of base stations is often the weakest part of the calculated network availability. Link redundancy, whereby base stations can be reached through backup links or routes using ring or meshed network topologies, can solve this. This section describes three methods to achieve link redundancy, including link switchover in the synchronous link domain, the use of standard IP routing protocols, and the use of Multi-Protocol Label Switching. Finally, some equipment reliability aspects are considered.

Self-recovery mechanism of SDH / SONET

Equipment on the basis of Synchronous Digital Hierarchy (SDH) or Synchronous Optical Networks (SONET) standards is often used for transport of E1 channels and IP packets. These backhaul networks rely on optical fibre or high bandwidth microwave links.

Redundancy in SDH / SONET networks can be achieved by means of redundant transmission paths using ring network topology. This self-recovery mechanism is illustrated in the diagram below.

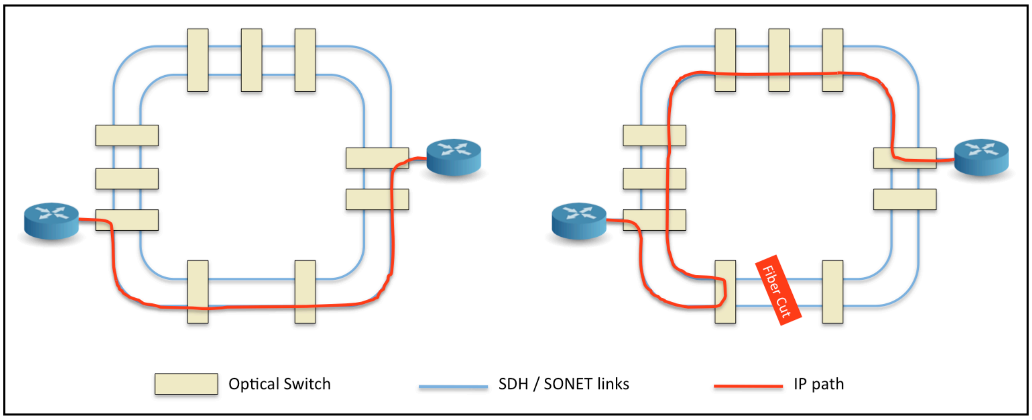

Figure 1 - Self-recovery mechanism within SDH / SONET networks

SDH / SONET networks use two sets of fibre optic links, one for sending and receiving, and the other as the spare set. If a fibre cut occurs, the switch on either side of the break re-routes the traffic in the other direction using the backup ring. Re-routing takes place at the physical layer, therefore the routers are not aware of the break and there is no need for corrective action by the routers. The failover takes less than 50 ms, with no noticeable impact on voice traffic or IP routes.

SDH / SONET networks can be used to carry IP packets by means of routers with the appropriate interfaces, as shown in the diagram above. Obviously, these networks can also be used to create E1 circuits for TDM based switching architectures, in which case no IP routers are required.

Re-routing in the IP domain

Self-recovery in the IP domain is possible using adaptive routing protocols. Well-known adaptive routing protocols include the Open Shortest Path First (OSPF) and Intermediate System to Intermediate System (IS-IS) protocols. The operation of adaptive routing protocols is illustrated in the diagram below.

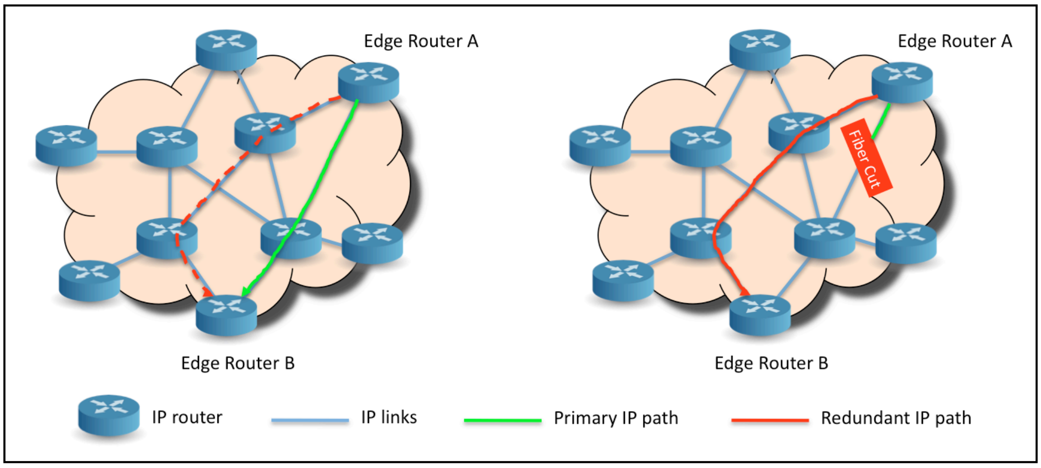

Figure 2 - Re-routing in the IP domain

The adaptive routing protocol finds the preferred transmission path automatically. In the above diagram, the shortest path is the primary IP path with the green colour. If the router discovers a break in the interconnection, a backup path is automatically discovered, as indicated in red. However, the detection of link failures and the negotiation between routers to establish a backup route typically requires several seconds, resulting in large numbers of dropped IP packets. The situation is even worse with intermittent link failures, causing the router to continuously switch between different paths.

The advantage of Multi-Protocol Label Switching

Multi-Protocol Label Switching (MPLS) combines fast re-routing capabilities with excellent Quality of Service (QoS) mechanisms.

MPLS meets the requirements for real-time applications with recovery periods of less than 50 ms, thanks to the fast re-routing capability of Traffic Engineering (TE). With Traffic Engineering, the primary and redundant paths are defined beforehand, enabling faster detection of link, port and node failures, and instant path switchover if failures occur. In addition, Traffic Engineering adds the capability to reserve bandwidth in order to provide robust Quality of Service.

Basically, the re-routing principles shown in figure 2 also apply to MPLS, but offer significant better resilience and Quality of Service compared to the standard OSPF and IS-IS routing protocols. Since MPLS is an open IETF standard supported by several leading suppliers of IP router equipment, it is considered the preferred solution to create carrier-grade all-IP networks.

Equipment reliability aspects

In addition to transmission link reliability, the equipment reliability should also be considered when determining the total availability of a TETRA network solution.

Equipment reliability is determined by the robustness of the hardware and software. Hardware reliability is determined by the Mean Time Between Failure (MTBF) figure of individual components, whereby extreme temperatures and mechanical stress can further deteriorate the reliability figures.

High software reliability is the result of high quality software engineering and comprehensive validation of functionality and performance using all possible network configurations. Networks should run reliably under high-load conditions, and cope with (intermittent) link and equipment failures that are out of control of the component running the software. In addition to the reliability of the system-specific software, the robustness and performance of the operating system should also be considered.

Equipment redundancy can help to increase the total system availability. Ideally, true no-single-point-of-failure may be provided, allowing automatic recovery of system operation whatever equipment or link failures occur. This can be further improved using geographic redundancy, offering protection against system failures due to extensive power outages (beyond the capacity of power backup facilities), fire and flooding.

Although no-single-point-of-failure may considerably increase system availability, it is also important to carefully consider the recovery time when failures occur. For example, if switchover to the redundant system takes a couple of minutes, it is very difficult to achieve ‘five-times-nine’ (99.999%) availability, which equals approximately five minutes of downtime per year.

It is clear that the total system availability is very much dependent on the system architecture and reliability of individual components within the TETRA solution. There is no simple rule to determine the expected availability. To help with the analysis of the equipment reliability, the following questions should be answered:

- Does the TETRA solution offer true no-single-point-of-failure?
- Which loss of functionality or capacity can be expected when switching over to a redundant component or system?
- What is the typical and guaranteed recovery time when switching over to a redundant component or system?
- What is the quality of the software with regard to exception handling and performance under high-load conditions?
- Are the hardware and operating system of carrier-grade quality with regard to stability, security and performance, also after several years of uninterrupted operation?

Scalability aspects

In general, scalability in TETRA networks involves two aspects, namely the size of the networks and the capacity (performance, throughput) of the networks.

Size of networks

TETRA networks may vary greatly in terms of sizing. A football stadium or small airport may be served by a single TETRA base station with just one carrier, whereas a nationwide network may require thousands of base stations with multiple carriers each.

Most TETRA solutions are limited in terms of scalability: either the network is designed for local or regional coverage with limited expandability, or the network is designed to provide large regional or nationwide coverage, which often makes the solution less competitive and too complex for small networks. Most important, limitations may be applicable which prevents expansion of an installed network, or require costly upgrades to different product lines.

Scalability limitations are mostly a result of the chosen system and network architecture. To satisfy the requirements for small networks, a simple architecture with a few components is preferred in order to reduce cost of investment, implementation and operation. Growth to large networks is usally limited due to capacity restrictions and availability issues of a single controlling node, or by issues with configuration, database synchronisation and switching when using a fully distributed solution.

Large networks can only be built by using a certain type of switching hierarchy. This mostly results in higher complexity of the system architecture, causing higher cost of investment, implementation and operation of the network.

Capacity of networks

Capacity is another scalability aspect, which should be dimensioned properly to provide sufficient performance in order to support the maximum expected call load and mobility of users within the network during peak hours.

Capacity requirements can be very different. For example, a TETRA system on a large airport requires high-load capacity using a single or just a few base station sites, whereas a rural area within a nationwide public safety TETRA network may be served with low capacity base stations, but with higher inter-site communication requirements as most calls involve multiple cells.

The following questions should be answered in order to evaluate capacity requirements:

- Does the controlling node, often referred to as Switching and Management Infrastructure (SwMI), offer sufficient call capacity in terms of calls per second and number of simultaneous voice and data calls during peak hours?
- Is the capacity of control channels and traffic channels sufficient to carry the expected amount of calls, also considering GPS location and application-generated data?
- Is the network architecture suitable and the capacity of links properly dimensioned to carry the expected amount of inter-site and inter-SwMI calls?
- Can the chosen system and network configuration cope with the expected future growth in call capacity and number of sites?

Evaluation of TETRA system architectures

In this chapter four existing TETRA system architectures are considered on the basis of the following three criteria:

- Is the solution future proof with regard to hardware, software and communication link requirements?
- Does the solution provide mechanisms for high availability, both in terms of base station link redundancy (such as IP/MPLS) and equipment redundancy?
- Is the solution scalable in terms of network sizing and call capacity?

The compatibility of solutions with Multi-Protocol Label Switching (MPLS) enabled IP backhaul networks is one of the key criteria of the evaluation, as MPLS is widely recognized as the preferred solution to build carrier-grade all-IP networks.

Hierarchical circuit switched networks

Networks based on hierarchical circuit switch technology use Time Division Multiplexing (TDM) switches and links. Components for TDM switching were developed in the 1970s and 1980s for traditional telephone exchanges according to SS7 and ISDN standards. The links between the switches and to the base stations are based on synchronous protocols, such as E1.

The TDM switches used in first-generation TETRA networks are often based on existing switching platforms, such as GSM switching platforms or large scale Private Branch Exchanges (PBXs). When properly designed, these networks can be scalable, reliable and resilient, as carrier-class telephony networks have to offer high capacity and require a high level of availability.

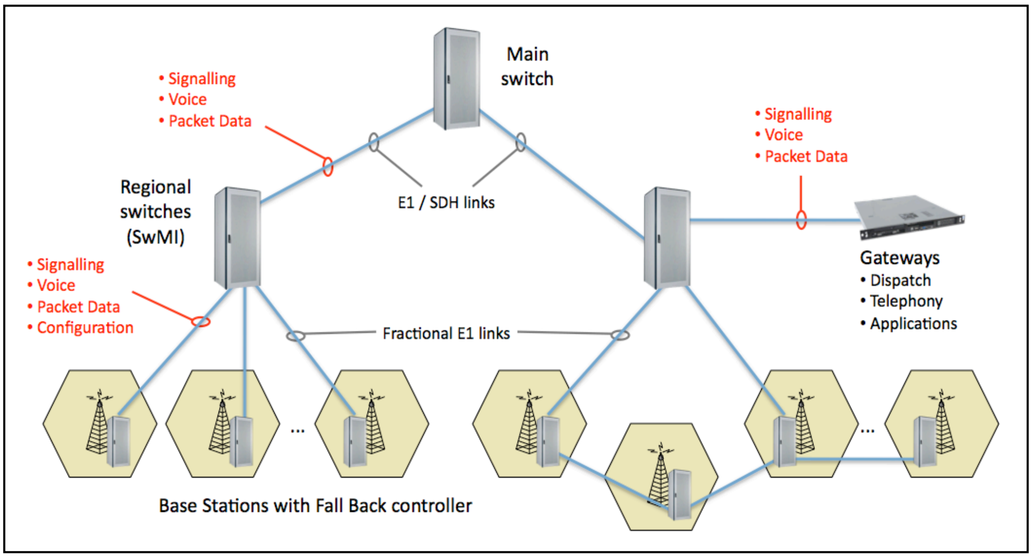

Figure 3 - Diagram of a hierarchical circuit-switched network

Although circuit switching is a proven and well-scalable technology, it is certainly not the optimal technology to build TETRA networks, for the following reasons:

- Traditional TDM switching technology requires many proprietary hardware modules, resulting in higher initial cost and cost of spares, a requirement for more rack space and higher energy consumption.

- The hardware modules are specifically designed and built for application in resilient switching networks. The availability of COTS components is therefore low, resulting in higher maintenance cost and component obsolescence issues.
- Complex hardware architecture also means complicated configuration and troubleshooting.
- The low-speed synchronous links (typically based on 64 kbit/s Signal Transfer Point (STP) links within the SS7 architecture) in between switching components limit the call setup performance of speech and data calls, especially when multiple switches are included in the end-to-end connection.
- TETRA Packet Data requires an overlay data network using additional router and gateway equipment, as traditional TDM switching in TETRA networks does not offer the capacity and flexibility to support multi-session TETRA Multi-Slot Packet Data.

Circuit switch based TETRA networks may be integrated with IP backhaul networks by means of TDM over IP. This involves a virtual link for transport of a TDM stream over an IP connection. This in turn requires a highly stable IP connection with low latency and sufficient bandwidth, but it may be more cost-effective compared to deploying traditional E1 links.

MPLS-based traffic engineering can also be used in combination with TDM over IP interconnection of base stations in order to benefit from base station link redundancy, as the necessary bandwidth from switch to base station is relatively static, and a limited number of routes through the IP/MPLS backhaul network has to be considered.

Hierarchical proprietary IP-based networks

Second-generation IP-based TETRA networks use proprietary equipment to meet requirements for mission-critical reliability and performance. The reason for this is the fact that in the late 1990s the IP standards and equipment were not mature enough to build core and backhaul networks with sufficient resilience. Some TETRA network suppliers therefore took the challenge to benefit from using the IP paradigm for TETRA networks by developing proprietary IP routing and multicast protocols that are specifically optimized for TETRA voice, data and signalling.

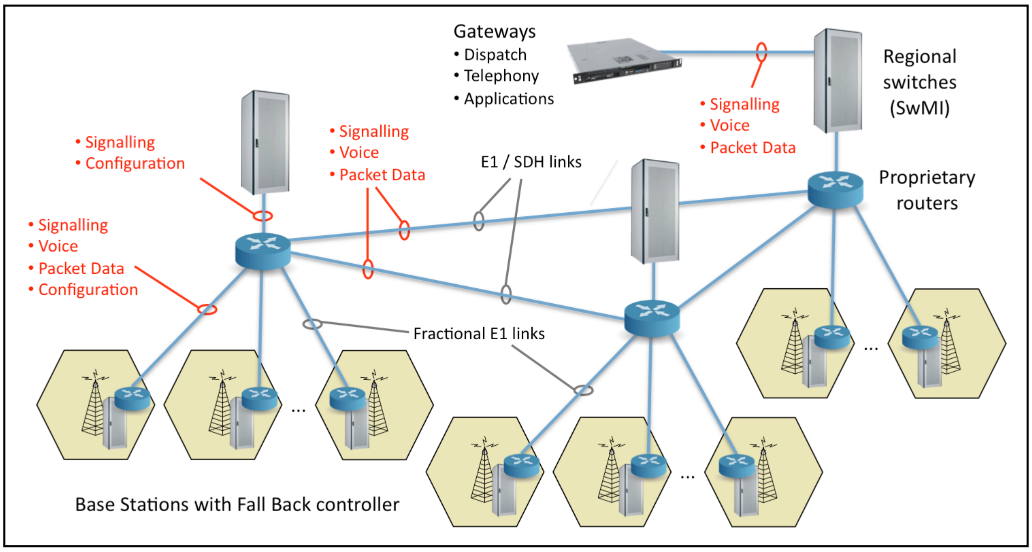

Figure 4 - Diagram of a hierarchical proprietary IP-based network

Packet switching of voice, data and signalling offers significant benefits in comparison with circuit switching, including a simplified architecture with less hardware components, more flexibility and integration opportunities, and fewer occurrences of component obsolescence.

On the other hand, proprietary elements in the core of the network and the use of dedicated routers diminish a part of the advantages as it involves higher equipment cost, higher maintenance cost and legacy issues when upgrading or expanding networks. Furthermore, these second-generation TETRA networks still tend to be complicated in terms of configuration and troubleshooting, since these networks consist of a multitude of servers, proprietary IP switches and routers. Each of these components has a specific function, such as voice and data routing, call management, network management, SDS gateway, dispatch server and packet data subsystem.

Redundancy is possible by adding redundant servers, IP equipment and links. However, due to the mixture of dedicated servers, IP switches and routers, redundancy becomes both complex and costly, and no-single-point-of-failure for all services with low switchover delay is very difficult to achieve.

Proprietary and open standards based IP routers are difficult to match. In the architecture shown before, the proprietary routers have to be complemented with open standards based edge routers in order to benefit from MPLS, basically duplicating router equipment. The necessary bandwidth to and from the base station is relatively static, and a limited number of routes through the IP backhaul network have to be considered, in order to benefit from base station link redundancy capabilities offered by MPLS-based Traffic Engineering.

It is worth mentioning that the proprietary IP architecture has proven to work for large-scale TETRA networks with over 3,000 sites and 50 regional switches, but still requires the E1 type of interconnection to base stations.

Fully distributed open IP-based networks

The promise of transparent communication through IP networks using Ethernet connectivity on IP routers has inspired a number of TETRA system suppliers to develop solutions based on a fully distributed IP network topology. By implementing the TETRA Switching and Management Infrastructure (SwMI) component on each site, a resilient network could be created, with unprecedented simplicity and low equipment cost.

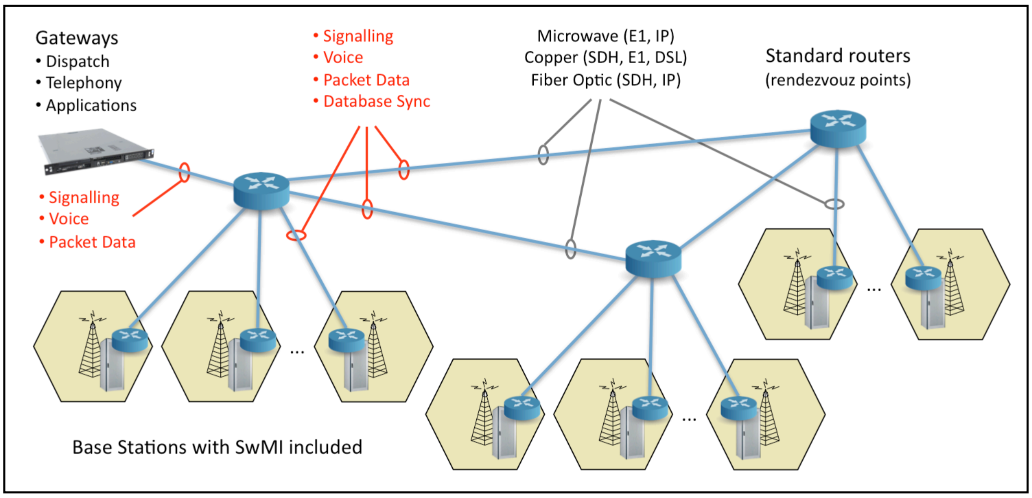

Figure 5 - Diagram of fully distributed open IP-based network

All known suppliers of TETRA networks in this category use standard IP routers, available from multiple vendors. Standard IP protocols such as the User Datagram Protocol (UDP) and Transmission Control Protocol (TCP), as well as the IP Unicast and Multicast protocols can be used to establish and maintain connections, to transmit speech and data, and to provide management functions. Low-cost, COTS router equipment can be used to interconnect the base stations over microwave, copper and fibre optic links. These routers also support the OSPF protocol for adaptive routing, but re-routing typically takes 2 to 30 seconds, which is not good enough to maintain calls. In addition, OSPF does not operate reliably with intermittent failing links.

Equipment redundancy can be easily achieved by duplicating the SwMI controller function, but it does not resolve the more important base station link redundancy issue. If a base station becomes isolated, the base station is of very little use as all communication to dispatchers and other sites is lost. No-single-point-of-failure thus requires redundant links as well, with sufficient capacity to carry all signalling, traffic and database synchronisation messages.

Unfortunately, additional challenges need to be met in order to create and maintain bigger networks, such as the requirement for reliability and speed of database synchronisation, status table updates for resource management, and the separate configuration of a large number of base station sites.

An important issue when using the fully distributed architecture in networks is the variation of bandwidth requirement, which is extremely difficult to predict. The required bandwidth is not just the total bit rate of the maximum number of simultaneous calls on the base station; the highly variable signalling (call setup and maintenance) as well as database synchronisation traffic also have to be considered. Especially the latter is difficult to predict, as each movement and status change of a radio in the network requires an update in all other sites and/or central database server(s).

Using IP Multicast may save bandwidth, but it involves additional difficulties in configuring equipment; it results in scalability issues (as mapping TETRA groups onto IP Multicast addresses limits the maximum number of groups), it is slow with regard to path reconfiguration, and IP Multicast alone does not meet the requirement for reliable transfer of database synchronisation messages.

MPLS-enabled router equipment may be deployed to benefit from fast re-routing capabilities, but here too the variable bandwidth requirement makes it difficult to perform Traffic Engineering, which has to be configured for a sufficient Peak Information Rate (PIR) in order to guarantee Quality of Service (QoS).

Softswitch open IP-based networks

The ever-evolving computing performance of standard IT technology has enabled the development of Softswitch-based technology. As software on top of COTS server hardware is used to perform all processing, switching and routing of TETRA speech and data, proprietary circuit switch hardware and proprietary IP-based router equipment are no longer needed.

The interconnection of systems and base stations through IP networks is a logical choice, since the COTS server equipment and operating systems support IP connectivity.

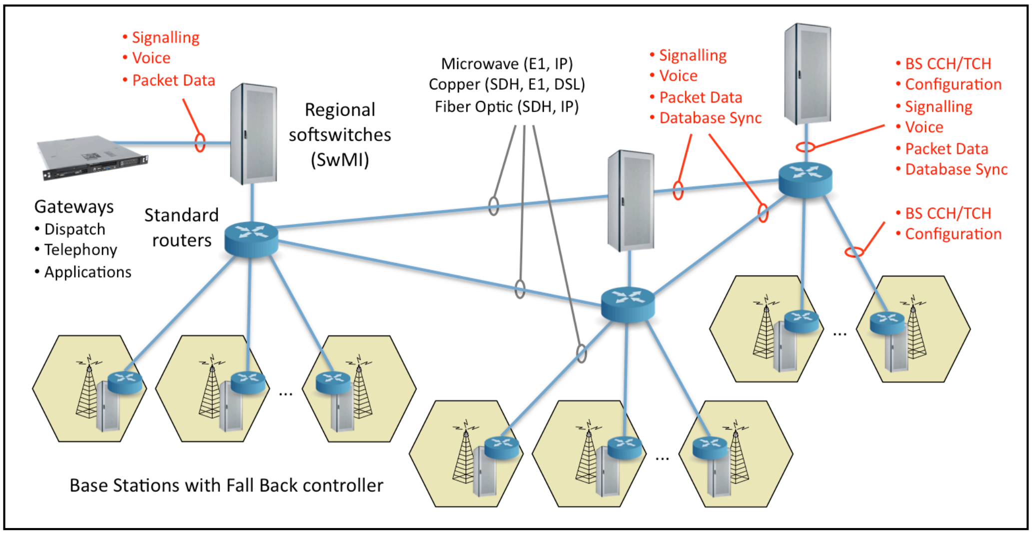

Figure 6 - Diagram of softswitch open IP-based network

Operation of softswitch technology has already been proven in many fixed and mobile telephony networks. In fact, almost all Voice-over-IP (VoIP) based PBXs and VoIP service providers use softswitch technology in their core networks, as do a growing number of mobile telephony providers.

Multi-vendor, open-standards based IP routers can be used in this type of system architecture, whereby standard IP protocols such as UDP and TCP, as well as IP Unicast and Multicast routing protocols can be used to establish and maintain connections, to transfer speech and data, and to provide management functions. Depending on the requirements for availability, a selection can be made from low-cost COTS router equipment that support the OSPF protocol, or more advanced MPLS-enabled routers to achieve the highest level of availability.

Equipment redundancy can be easily achieved by duplicating the softswitch, either on a single location by means of co-located redundant hardware, or on a physically different location, providing geographic redundancy. Due to the significant lower cost of COTS hardware in comparison to circuit switch and proprietary IP-based equipment, the additional expenses for equipment redundancy are kept to a minimum.

For maximum availability, redundant links should be considered from the main and redundant softswitch to each of the base stations. Since no IP multicast is used in between the softswitch and the base station, and configuration of the base stations is performed on the softswitches only, the configuration complexity is significantly reduced.

On a higher level, the communication between softswitches is based on the same principles as those described for the fully distributed network topology. These inter-SwMI links carry the signalling, voice and data, and database synchronisation messages. However, since a softswitch serves an entire city or region and mobility is concentrated in the area served by the softswitch, the amount of communication in between softswitches is much less. The result is less (variation of) bandwidth in between the SwMIs compared to “Fully distributed open IP-based networks”.

The bandwidth of communication between the softswitch and the base station is static. Besides, a limited number of alternative routes have to be considered for link redundancy. Both aspects help to get maximum benefits from fast re-routing capabilities offered by IP/MPLS-based Traffic Engineering.

Softswitch technology also opens the opportunity to integrate different subsystems with the core switching and routing functions for TETRA voice and data. Obviously, the softswitch also performs the call and resource management functions. In addition, network management, databases, SDS gateway, packet data and even TETRA protocol stacks may be integrated within a single softswitch application. This potentially eliminates the need for multiple physical servers or hardware virtualization, which often present challenges in terms of reliability and manageability.

Regarding scalability, today’s softswitching architecture offers a capacity and performance similar to that of hierarchical proprietary IP based networks. At the same time, it requires less hardware equipment, involves virtually no legacy / component obsolescence issues, it offers simpler redundancy concepts and is (much) easier to configure and troubleshoot. Ultimately, this results in higher availability, combined with lower investment, lower implementation and lower operating costs.

Conclusion

Over a period of more than 10 years, more than thousand TETRA networks have been deployed worldwide for a wide range of applications in the military, public safety, transport, oil & gas and industry market segments, using different approaches regarding system architecture and network topology.

Since TETRA networks can vary in size from a single base station to a nationwide network, the challenge is to select an architecture that is easy to scale to facilitate expansion of coverage and capacity during the lifetime of the network on the basis of one single, consistent solution.

Various different system architectures and topologies for TETRA networks exist today, the strengths of which are well promoted by the respective suppliers. Obviously, the weaknesses are not so much highlighted. An objective comparison between architectures should allow for a better selection of the right supplier of equipment and services.

Glossary

ATM	Asynchronous Transfer Mode
COTS	Commercial Off The Shelf
DSL	Digital Subscriber Line
FR	Frame Relay
FTTH	Fibre To The Home
GPS	Global Positioning System
GSM	Global System for Mobile Communication
IETF	Internet Engineering Task Force
IP	Internet Protocol
IS-IS	Intermediate System – Intermediate System
ISDN	Integrated Services Digital Network
ISP	Internet Service Provider
IT	Information Technology
MPLS	Multi Protocol Label Switching
MTBF	Mean Time Between Failure
OSPF	Open Shortest Path First
PBX	Private Branch Exchange
PIR	Peak Information Rate
POTS	Plain Old Telephone System
QoS	Quality of Service
SDH	Synchronous Digital Hierarchy
SDS	Short Data Service
SONET	Synchronous Optical Networking
SS7	Signalling System 7
SwMI	Switching and Management Infrastructure
TCP	Transmission Control Protocol
TDM	Time Division Multiplexing
TE	Traffic Engineering
TETRA	Terrestrial Trunked Radio
UDP	User Datagram Protocol
UMTS	Universal Mobile Telecommunications System
VoIP	Voice over IP
WAN	Wide Area Network

The use of Wikipedia is highly recommended for a detailed description of the terms and abbreviations listed above.