

paper

## Seven reasons to use end-to-end thinking when building all-IP networks

Most mobile operators around the world are already well on their way to all-IP networks. Their concern now is how to complete that transition and handle the substantial growth now being seen in mobile broadband services. They can address these concerns by choosing an end-to-end IP transport solution.

white

# Introduction

The benefits of an all-IP network are clear. Ethernet-based IP transport, for example, reduces costs and enables service to all users, from low-revenue voice-plan-only users to intensive users of high-speed data services. Security and QoS (quality of service) can be built in as part of the network design, providing resiliency and high availability on a par with traditional circuit-switched telephony networks. An all-IP network meets future requirements, solving data and capacity bottlenecks and preparing the way for the Evolved Packet System (LTE and SAE).

The question many operators face is how to make an efficient transition from their current voice-centric transport infrastructures to a fully packet-data-centric model. Each operator is starting from a different position. Many mobile operators' networks have been built in an ad-hoc manner or grown through acquisition, resulting in high opex, lower reliability and increased round-trip delay. In the core network, for example, many

operators already have some IP infrastructure deployed to deliver GPRS traffic but this has not been updated sufficiently. This infrastructure often uses older technology and prevents operators from gaining the full benefit of their IP investments.

Operators are advised to take an end-to-end approach. This means taking a holistic view of both service requirements and how these requirements affect the structure, technology and network components of the optimal solution for each part of an operator's network. When possible, operators should choose a single vendor that understands the entire network from a telecom perspective and can deliver telecom-specific goals such as high capacity, security, QoS, manageability, resilience and a future-proof migration path. Building an all-IP network is more than simply connecting a number of routers, switches and firewalls.

# Mobile network overview

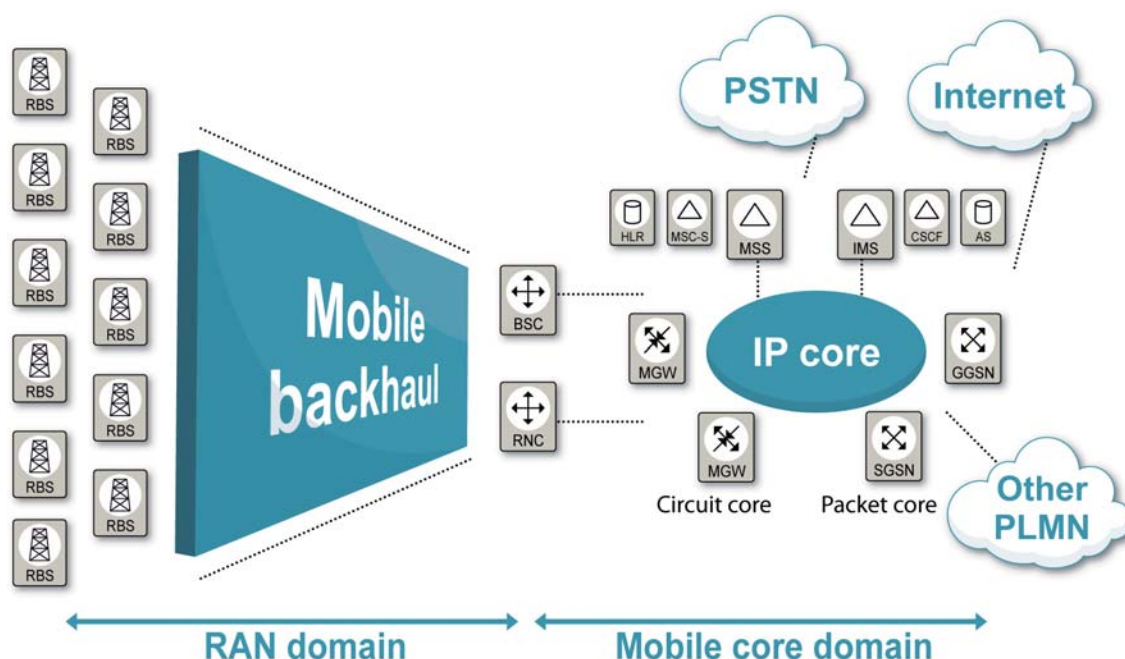


Figure 1: Mobile network functional segmentation

Before analyzing the benefits of an end-to-end solution, it is worth defining the parts of the mobile network and how they interact with each other.

The entire infrastructure of a typical mobile operator can be divided into several distinct parts.

**RAN Domain:** This is the access/aggregation part, funneling traffic from a large number of RBSs towards a much smaller number of RNCs (for WCDMA traffic) or BSCs (for GSM traffic). Voice traffic is directed towards the core network via Media Gateways (MGW) whereas packet-data traffic is directed towards SGSNs and GGSNs.

**Mobile core domain:** The core network sits between the radio access networks and external networks such as the internet, PSTNs and other mobile operators. It contains the serving nodes (SGSNs and

GGSNs) controlling data sessions and traffic forwarding as well as MSC and MGW functionality for providing call switching and associated services.

**Mobile backhaul:** Within the RAN domain, the mobile backhaul takes care of transporting traffic between the RBS and BSC and/or RNC sites. There are many ways in which an operator can do this, and the RAN solution should be independent of the transport method chosen. Possible transport networks include L2 networks (Carrier Ethernet), L3 networks (BGP/MPLS L3 VPN) and IP over E1/T1 using MLPPP.

In cases where the chosen transport network is not immediately available at the RBS site, last-mile access must also be considered. Possible solutions for this include microwave, copper and optical fiber (FTTx).

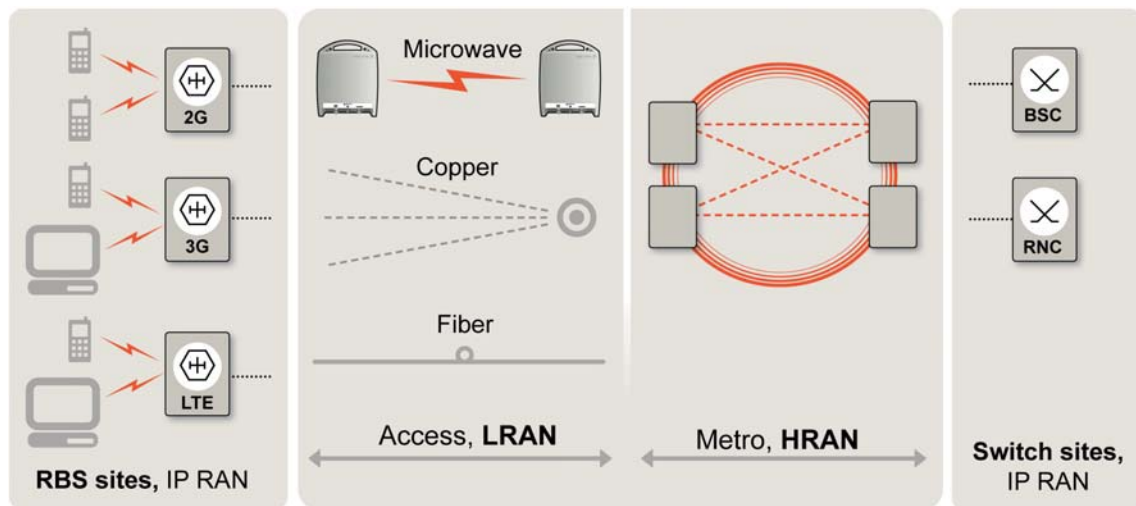


Figure 2: Mobile backhaul for the radio access network

Mobile backhaul can be divided into the “low” and “high” RANs (LRAN, HRAN) reflecting the asymmetrical nature of backhaul networks, in which a large

operator could have a huge number of RBS sites concentrated towards a much smaller number of switch (RNC/BSC) sites.

# Reason 1: reduced opex, capex and TCO

An all-IP network will mean significant savings for an operator's bottom line. IP-based transport is not only cheaper on a bit-per-second basis but is more easily scaled, which allows operators to better accommodate the growing demand for higher bandwidth. The simplicity of the Ethernet solution also reduces management and deployment costs substantially.

There is obvious potential for considerable cost reduction but how can an operator best exploit it?

With a holistic approach, operators and system integrators evaluate every network element as well as the management systems that make up the entire communication chain. The optimal solution should be designed to scale and adapt easily. The operator will need to get all the elements

working together efficiently, from the radio access through the backhaul to the core network. This should be done with the minimum of overlap or underutilized infrastructure.

An end-to-end approach will:

- Use common platforms and technologies for both the radio-access and core-network elements to minimize both capex and opex as well as enable faster integration
- Reduce capex by replacing existing multiple-transport networks with a single integrated IP network
- Achieve lower total cost of ownership (TCO) for the backhaul through efficient aggregation regardless of the physical infrastructure used (optical, copper or microwave media).

# Reason 2: shorter time to market and more efficient use of current infrastructure

Getting products and services to the market first is the aim of any efficient business organization. However many operators have inflexible networks and management systems that hinder rather than support the launch of new services. Missing a market window due to rollout delay or failure can have serious consequences for an operator's revenue stream.

Operators need a network solution that is verified and proven – one that has undergone lab testing as well as integration testing with the core network, radio-access-network equipment and other appropriate services. This approach should also look at the existing network and allow operators

to maximize their investment in the existing systems.

No two operators are alike but one thing is common to all: the need both to maintain their ongoing business throughout a network transformation, and to reduce costs by utilizing the current infrastructure as much as possible. An end-to-end solution should be implemented in step with an operator's changing needs and business plan; investments must be made when they make sense.

An end-to-end approach will:

- Utilize network and service-management systems that can simplify the launch of new services by simplifying customer

- handling, service provision and resource management
- Allow the backhaul network to evolve to IP RAN when the capacity requires it
- Allow operators to use their existing transport networks, previously used for TDM, to transfer IP packets between the RBS and BSC/RNC sites. In this way, an operator planning to move to IP can start the migration process by deploying an all-IP network on its legacy infrastructure
- Be standards-based for successful interoperability with existing network equipment and transport services.

## Reason 3: increase network security

Security is a growing issue for carriers and operators. As mobile networks continue their evolution toward all-IP, it is crucial to consider network-wide security at the planning stage, rather than as an afterthought. Increased connectivity thanks to the possible use of public networks for backhaul and increased adoption of native IP devices both make networks more vulnerable.

A comprehensive security policy – developed according to the security needs of the operator – should be a central pillar of any end-to-end approach. In the network, a risk analysis will be made for every node and traffic type. Separate security zones will be created within and between sites and then protected according to their assessed risk levels.

In the radio access network, increased RBS connectivity as well as insecurity in the

transport network (sometimes using public or semi-public networks) are the two main causes for concern. It is much more difficult to add security after the network is operational, and this may require a major network redesign.

An end-to-end solution will:

- Build on a strong set of basic security features and inherently secure products that help operators lower their capex by having fewer dedicated security nodes and lower their opex by reducing the need for administrative processes
- Allow basic or advanced levels of protection according to the types of services provided and the operator's security policies
- Ensure that every element in the network can survive a denial of service (DoS) attack.

# Reason 4: guaranteed quality of service (QoS)

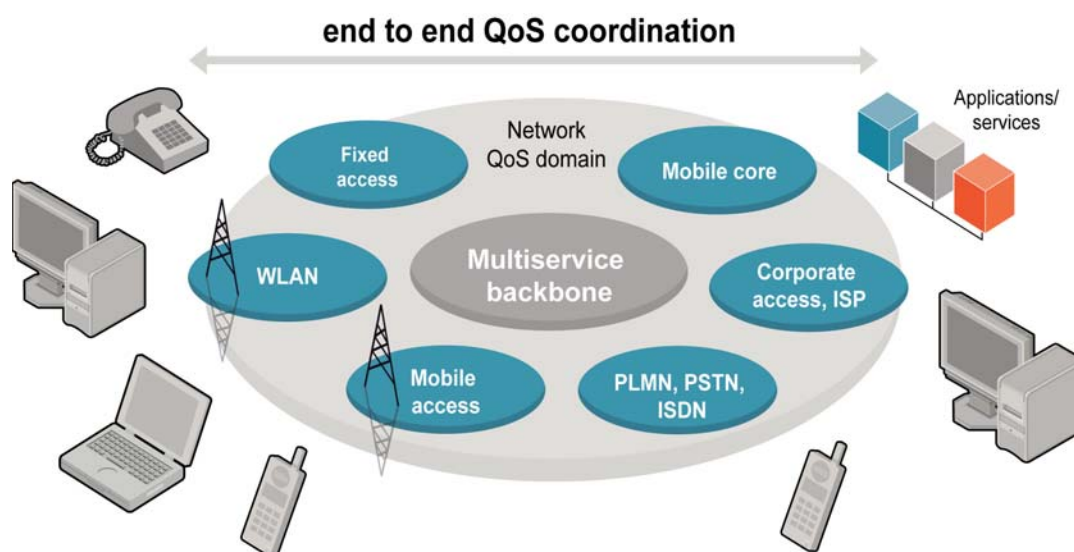


Figure 3: Guaranteeing end-to-end QoS across multiple network domains

QoS is the ability to guarantee a certain level of performance for traffic through the network, including throughput, delay, delay variance and reliability.

Different traffic types require different levels of QoS. For instance, network control and management traffic will place high demands since the network depends on them, whereas best effort data traffic such as web browsing could have substantially reduced priority. Without a well defined QoS policy, an operator's network will function much less efficiently, creating delays in time-sensitive services and resulting in dissatisfied consumers. QoS can conversely be a revenue generator, as consumers become willing to pay for better QoS such as tiered services or guaranteed throughput levels.

An end-to-end approach will ensure QoS requirements are already fulfilled at the planning stage. The solution consists of QoS mechanisms in mobile terminals, radio access networks, core network, service network and IP backbone. QoS functionality in gateway nodes enables interworking with other external networks. The solution will encompass all network layers from top to bottom, as well as every network element from an end-to-end perspective.

An end-to-end approach ensures telecom-grade QoS by using:

- Network dimensioning – including a detailed inter-site traffic matrix for the different traffic-class types. The network-dimensioning process results in bandwidth in the network being provisioned according to transport needs.
- Traffic differentiation – determining as a first step all traffic types traversing the network. Those traffic types can then be grouped based on the delay sensitivity of the traffic.
- Queuing and scheduling – determining the order of transmitting packets of the forwarding classes on the outgoing interfaces. Each router and switch will implement internal queuing and scheduling algorithms to ensure the QoS of the different traffic.
- Admission control – required to ensure that infrastructure capacity is not overloaded. Mobile nodes, such as the MGW, will limit the traffic injected into the backbone network, thus maintaining voice quality when there is congestion in the backbone network. The network will therefore behave in the same way as traditional TDM-based networks when congestion occurs.

# Reason 5: high availability

Traditionally, IP-based networks had a reputation for failing to meet the high reliability standards associated with TDM and ATM networks. However improvements in IP-network-node software and hardware has made goals such as 99.999 percent uptime possible, as well as quick failover to redundant network paths in case of any single failure in the network.

The key to building resilient networks is to understand that reliability must be supported by all the network elements, from the services and applications right down to the platforms upon which the network operates.

All nodes (mobile nodes as well as IP-network nodes) included in the packet transport will have built-in resiliency mechanisms, some using standard routing protocols, some using built-in application-based resilience mechanisms and others using host-based resiliency mechanisms. It is not always easy to understand which mechanisms to choose to achieve the best possible result in a large network with many traffic types and traffic nodes.

To succeed, it is vital that an end-to-end approach is taken right from the beginning. It is also important to understand what the exact network requirements are – for instance, how quickly a failover between two paths needs to be carried out to guarantee that users will not be affected.

An end-to-end approach will ensure:

- High availability of individual nodes – achieved through hardware redundancy and an operating system designed for high reliability
- Redundancy of nodes and links – a network designed so that no individual link or node failure can prevent traffic from reaching its destination
- Mechanisms for rapid detection of path failure, and mechanisms for rapidly moving traffic onto alternative paths such as routing protocols, host resilience mechanism and protection protocols in the backbone network
- Security – because many network failures are caused by a lack of sufficient security, leaving them vulnerable to DoS attacks and similar threats.

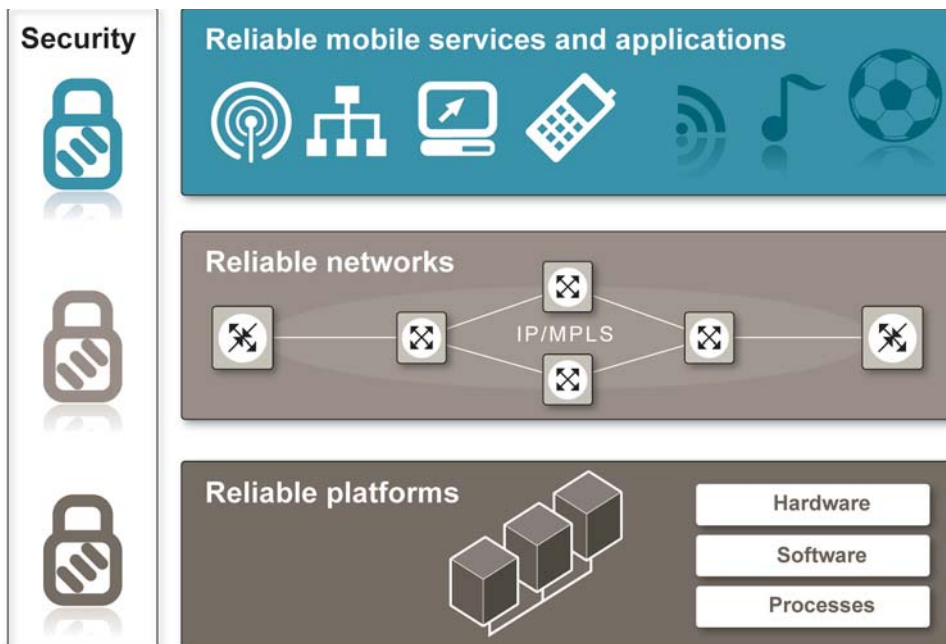


Figure 4: Reliability and security place demands at every level

## Reason 6: assured migration path

When it comes to any technology, knowing what is around the corner is never easy. In the telecom world the situation is made somewhat clearer through agreed standards that map out the progression and evolution of the mobile network. In the coming few years, both GSM/UMTS and many CDMA operators will move to the new mobile standards known as Long Term Evolution (LTE) and System Architecture Evolution (SAE). LTE will have significant benefits over today's networks including more efficient use of the radio network, faster transfer rates, higher mobility and lower latency.

By adopting an end-to-end methodology when moving to an all-IP network, operators can better prepare themselves for the future steps that will be needed when moving to LTE/SAE. Operators can now take

intermediate steps towards the 3GPP standards for SAE and the Evolved Packet Core (EPC) – the specification for changes to the packet-core network architecture. These can improve network scalability, make future expansions more cost-effective and reduce transmission costs.

An end-to-end approach will:

- ❖ Minimize future capex and opex by defining clearly where investments should best be made to meet the future needs of LTE/SAE
- ❖ Make sure infrastructure is capable of supporting the connectivity and capacity requirements of the future (high-density gigabit Ethernet, scalability, forwarding performance, advanced services – deep packet inspection, policy, subscriber management and so on).

## Reason 7: more powerful and efficient network management

It is clear that any network transformation should be matched by a corresponding network-management transformation. Management transformation can help decrease costs, ensure high-quality service delivery to customers, maximize revenues and establish a sound foundation when moving to next-generation networks and services.

An end-to-end approach will help create effective management systems and processes across the entire network; this will enable operators to attract and retain customers. It will also increase operational readiness, allowing a shorter time to market for new products and technologies.

An end-to-end approach will:

- ❖ Monitor key performance indicators (KPIs) to guarantee the health of the network and track key criteria such as network loading. This ensures that capacity planning is effective and that service-level assurances are met for both contractual purposes and end-user service satisfaction
- ❖ Automate some network-deployment functions with auto-configuration, common configuration templates and the simplification of complex tasks such as MPLS LSP configuration
- ❖ Simplify management systems by incorporating capabilities within each network domain by utilizing a network-domain manager to make the capabilities and features of each network domain available to all other management domains
- ❖ Reduce dependency on stand-alone vertical systems
- ❖ Reduce operational expenses and move to cost-effective, integrated management based on an architecture with clear roles, responsibilities and interfaces between management domains.

# Conclusion

Transition is never easy. Operators today face transition not only in their networks and management systems but also in their organization and processes. Transition, however, can be made easier if an operator knows where it wants to go and can take a comprehensive view of its entire business and network landscape.

This requires an IP-infrastructure solution that is coherent, reliable and cost-effective. A new network must be able to accommodate enormous growth in broadband packet data, largely driven by video or multimedia, and be capable of continuing the evolution to all-IP and the Evolved Packet System (LTE/SAE) without extensive reevaluation and investment.

Choosing a single vendor with expertise in all the elements of the mobile network can bring enormous benefits. A single vendor can

provide guidance for the entire network, and its professional services staff can help analyze, identify and recommend when to increase backhaul capacity, when to aggregate traffic, and which ATM or TDM components should be replaced with IP-over-Ethernet components and when.

Telecom quality is the fundamental differentiator. It is not only about reliability but also standards compliance and a commitment to support solutions as entities rather than a collection of boxes. Solutions must have committed roadmaps, development teams and dedicated support. This is why it is essential to partner with a major telecom industry player that understands and is helping shape future mobile industry standards, and can guide operators through the challenges ahead.

# Glossary

<b>2G</b>	second-generation radio technology for wireless networks	<b>PLMN</b>	public land mobile network
<b>3GPP</b>	3rd Generation Partnership Project	<b>PSTN</b>	public switched telephone network
<b>3G</b>	third-generation radio technology for wireless networks	<b>QoS</b>	quality of service
<b>AGW</b>	application gateway	<b>RAN</b>	radio access network
<b>ATM</b>	Asynchronous Transfer Mode	<b>RBS</b>	radio base station
<b>BGP</b>	Border Gateway Protocol	<b>RNC</b>	radio network controller
<b>BSC</b>	base station controller	<b>SAE</b>	System Architecture Evolution
<b>BSS</b>	business support systems	<b>SGSN</b>	Serving GPRS Support Node
<b>capex</b>	capital expenditure	<b>SLA</b>	service level agreement
<b>CDMA</b>	code division multiple access	<b>TCO</b>	total cost of ownership
<b>DRM</b>	digital rights management	<b>TDM</b>	time division multiplexing
<b>DoS</b>	denial of service	<b>UMTS</b>	Universal Mobile Telecommunications System
<b>DPI</b>	deep packet inspection	<b>VPN</b>	virtual private network
<b>EPC</b>	Evolved Packet Core	<b>WCDMA</b>	Wideband Code Division Multiple Access
<b>FTTx</b>	Fiber to the x, where x can be N (node), C (curb), B (building) or H (home)	<b>WLAN</b>	wireless local area network
<b>GGSN</b>	Gateway GPRS Support Node		
<b>GPRS</b>	General Packet Radio Service		
<b>GSM</b>	Global System for Mobile communications		
<b>HRAN</b>	high radio access network		
<b>HSPA</b>	High Speed Packet Access – part of 3GPP WCDMA standard		
<b>IP</b>	Internet Protocol		
<b>ISDN</b>	Integrated Services Digital Network		
<b>ISP</b>	internet service provider		
<b>KPI</b>	key performance indicators		
<b>LRAN</b>	low radio access network		
<b>LSP</b>	Layered Service Provider		
<b>LTE</b>	Long Term Evolution		
<b>MGw</b>	Media Gateway		
<b>MLPPP</b>	Multi link Point-to-Point Protocol		
<b>MPLS</b>	Multiprotocol Label Switching		
<b>MSC</b>	mobile switching center		
<b>opex</b>	operational expenditure		
<b>OSS</b>	operations support systems		

# References

- Ericsson AB, Ericsson Review 2004. *Modularity is key when designing packet backbone networks for mobile services*. Available at: [http://www.ericsson.com/ericsson/corpinfo/publications/review/2004\\_01/182.shtml](http://www.ericsson.com/ericsson/corpinfo/publications/review/2004_01/182.shtml) [Accessed 12 January 2009].
- Ericsson AB, Ericsson Review 2004. *Security architectures for mobile networks*. Available at: [http://www.ericsson.com/ericsson/corpinfo/publications/review/2004\\_02/191.shtml](http://www.ericsson.com/ericsson/corpinfo/publications/review/2004_02/191.shtml) [Accessed 12 January 2009].
- Ericsson AB, Ericsson Review 3 2008. *Mobile broadband backhaul: Addressing the challenge*. Available at: [http://www.ericsson.com/ericsson/corpinfo/publications/review/2008\\_03/](http://www.ericsson.com/ericsson/corpinfo/publications/review/2008_03/) [Accessed 12 January 2009].
- Ericsson AB, white paper. March 2006. *Telecom quality in all-IP networks*. Available at: [http://www.ericsson.com/technology/whitepapers/3063\\_Telecom\\_Quality\\_all\\_IP\\_B.pdf](http://www.ericsson.com/technology/whitepapers/3063_Telecom_Quality_all_IP_B.pdf) [Accessed 12 January 2009].
- Ericsson AB, white paper. October 2008. *High speed technologies for mobile backhaul*. Available at: [http://www.ericsson.com/technology/whitepapers/broadband/high-speed\\_mobile\\_backhaul.shtml](http://www.ericsson.com/technology/whitepapers/broadband/high-speed_mobile_backhaul.shtml) [Accessed 12 January 2009].