Auxiliary ANNEX E

Detailed Technical Descriptions

Table of contents

Table of Figures

Table of Tables

1. Architecture of Future Networks

The architecture of future networks is described in this section to help clarify its basic structure and components.

The concept of the future networks' architecture is shown in the figure below (see Figure 1). The wireline and wireless terminals are connected to the core transport through an access layer. The session and control layers control all other layers such as application, transport and access. As shown in the figure, the application layer can be unbundled from the underlying transport and access layers using open and standardised interfaces. This allows future networks to be easily connected to other networks (e.g., the Public Switched Telephone Network (PSTN)[1]) via gateways, thus allowing different types of data to flow seamlessly through the networks.

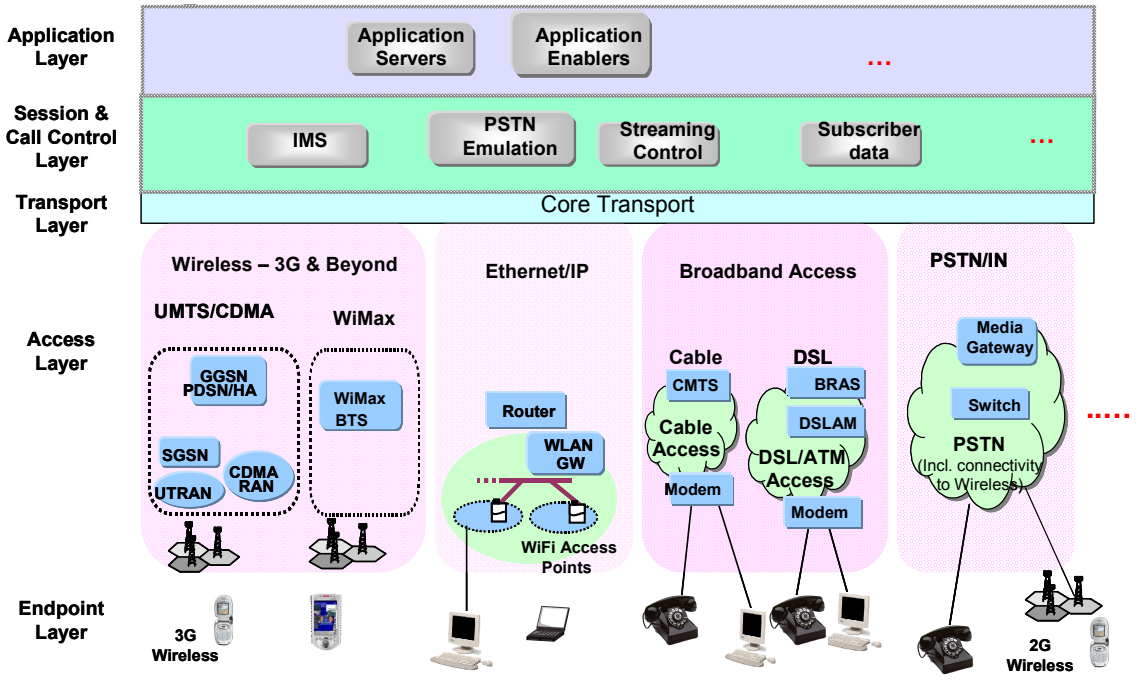


Figure 1: The Architecture of Future Networks

1.1. Major components of Future Networks

In addition to the traditional voice and data equipment, the architecture for the future networks contains converged network equipment types such as Session Controllers or Call Controllers (e.g., in Internet Protocol (IP) Multimedia Subsystem (IMS)), Media Gateways, Signalling Gateways, Feature Servers, Application Servers, Media Servers and Management Servers, along with Provisioning and Billing Interfaces. Core technologies include packet transmission technology, traffic engineering control protocol, technology that guarantees

1 In this document the term PSTN includes POTS and ISDN unless there is a particular issue to be highlighted.

quality of service (e.g., Multi Protocol Label Switching (MPLS)) multi-party telecommunications technology (e.g., real-time multicasting), and session control technology.

The following glossary describes key network elements[2] that are common to one or more of the future network architectures (e.g., 3G, WiFi, cable). Subsequent sections will provide additional network specific elements definitions. It is important to note that the future network allows for network functionality to be partitioned differently. As such, different vendors may partition the same functionality across different network elements

- **AS:** The Application Server (AS) provides control for services, and is accessed by interacting with the Call Session Control Function (CSCF) or directly with the user. The AS may reside either in the user's home network or in a Third Party location. The AS may consist of SIP AS, Open Service Architecture (OSA) AS, and Intelligent Network (IN) AS connected via a Service Switching Function (SSF). The SSF provides access and inter-working to a legacy IN Switching Control Point (SCP). The AS does the following:
  - It executes service logic based on the subscriber's service profile and on the terminal capability (device profile).
  - It inter-works with other application servers, such as a presence server, geographical information systems (GIS) server, or another AS, to provide convergent services to the end user.
  - It interacts with the Access Gateway Control Function (AGCF) directly or through the CSCF to communicate with PSTN/IN users.
  - Examples include call feature application servers, presence servers, various messaging servers, conference servers, home application servers, etc.
- **BG:** The Border Gateway (BG) is a gateway between a Public Land Mobile Network (PLMN) supporting GPRS and an external inter-PLMN backbone network used to interconnect with other PLMNs also supporting GPRS. The role of the BG is to provide the appropriate level of security to protect the PLMN and its subscribers.
- **BGCF:** The Breakout Gateway Control Function (BGCF) determines the PSTN/IN network to which a call will be routed by selecting the corresponding Media Gateway Control Function (MGCF).
- **CE Router:** Customer Edge (CE) router is a logical endpoint router connected to an MPLS network. In most cases, any router can be used as a CE. No MPLS-specific function is needed.
- **CMTS:** Cable Modem Termination System (CMTS) is essentially a router that supports Radio Frequency (RF) interfaces to connect to the cable modems over the cable plant. Thus, the CMTS connects the Cable plant to the IP network.
- **CSCF:** The Call Session Control Function (CSCF) is the central call processing entity for calls. It can function in three modes: Serving, Proxy, and Interrogating. It handles functionality related to session control, e.g., registration, origination of sessions (session setup, modification, and teardown), and routing of session messages. It interacts with the ASs to trigger requested services. It processes requests from users (and terminals) for registration and can route messages to terminals based on the routing (location) information obtained at registration. It interacts with the AGCF to communicate with PSTN/IN users.

2 To prevent Figure 1 from becoming too busy not all these elements are shown there. These network elements are common to the future network technologies described in subsequent sections and are collected in this section to facilitate the reader.

- **DHCP server:** Dynamic Host Configuration Protocol (DHCP) server is used by (access) service providers to distribute IP addresses to its endpoints (e.g., cable modems) from the IP address pool of the service provider.
- **DNS server:** Domain Name System (DNS) servers are used primarily for mapping host names including Fully Qualified Domain Names (FQDNs) to IP addresses. DNS functions have been generalised to mapping of other addressing entities. For example the, ENUM function maps a telephone number to the location of the endpoint's domain (which then gets mapped to the IP address of the endpoint).
- **DSLAM:** DSL Access Multiplexer (DSLAM) multiplexes connections to multiple Digital Subscriber Line (DSL) modems for connecting to an IP network, usually through an Asynchronous Transfer Mode (ATM) switch.
- **Ethernet Switch:** Supports IP endpoint Ethernet connectivity in Local Area Network (LAN) and increasingly in Wide Area Network (WAN). This is Layer 2 switching over a "broadcast domain" of endpoints. An Ethernet switch or a network of Ethernet switches can support multiple broadcast domains called Virtual Local Area Networks (VLANs).
- **Firewall:** A set of security functions implemented to allow or deny certain traffic (defined by policies) in parts of the network being protected. The firewall can be a stand-alone product. Many router products provide firewall functions that are more sophisticated than traditional Access Control Lists (ACL).
- **Frame Relay / ATM Switch:** Basic network elements in a Frame Relay or ATM network respectively.
- **(Media) Gateways:** Service providers must provide connectivity to their legacy services, such as PSTN/IN and legacy endpoints (e.g., Public Branch Exchange (PBX) and analog telephones). A gateway supports connectivity to IP network on one side and interfaces to legacy networks on the other. A gateway can be as simple as a telephone adapter connecting an analog phone to a cable or DSL modem or a more complex media gateway connecting many Primary Rate Interface (PRI) or Integrated Service Digital Network Users Part (ISUP) trunks to a PSTN/IN circuit switch carrying traffic for a large number of voice calls.
- **IDS:** Intrusion Detection System (IDS) is a device or set of devices that report on certain harmful and unwanted traffic streams (defined by policies). Some IDS systems can additionally prevent such traffic streams from entering the protected parts of the network. In addition to stand-alone IDSs, some firewall and router products support IDS functions as additional capabilities.
- **Layer 3 Switch:** This is an evolution of a network element that provides both the Ethernet switching and IP routing functions.
- **MG:** The Media Gateway (MG) provides inter-working between the packet-based transport used in the future networks and trunks from the circuit-switched network. It is under the control of the MGCF. It may support payload processing (e.g., codec's and echo cancellers).
- **MGCF:** The Media Gateway Control Function (MGCF) controls the MG to provide inter-working with PSTN. It processes and forwards requests from the Signalling Gateway to the CSCF. It may include an IN mediation function (i.e. an SSF) in order to provide services for legacy IN applications.

- **MRFC:** The Multimedia Resource Function Controller (MRFC) controls the media stream resources in the MRFP. It interprets information coming from an AS and S-CSCF and controls the MRFP accordingly.
- **MRFP:** The Multimedia Resource Function Processor (MRFP) provides resources to be controlled by the MRFC. The resources include mixing of incoming media streams (e.g., for multiple parties), sourcing of media streams etc.
- **PDF:** The Policy Decision Function (PDF) acts as a policy decision point for service based local policy control of IP bearer resources. The PDF makes decisions about IP bearer resource allocation requests.
- **PE Router:** Provider Edge (PE) Router, also called Label Edge (Router), is the MPLS network access router to which the CEs connect.
    - Routers within the MPLS network that do not support the PE function are called Label Switching Routers (LSR).
    - Many router products support additional functions required of them to act as a PE and an LSR.
- **Router:** The basic network element of Internet Protocol (IP) networking. It performs most functions at Layer 3 of the Open System Interconnection (OSI)[3] model. Most router products support many routing protocols, many physical and logical connectivity options, and Access Control Lists (ACLs) for packet filtering and route filtering security functions.
- **SBC:** Though not strictly an IP networking product, a Session Border Controller (SBC) is deployed at the border of interconnecting Voice over IP (VoIP) domains or isolates a VoIP domain from the IP network. An SBC provides one or more of the following functions: Firewall, Application Layer Gateway that provides deep packet inspection for VoIP signalling and bearer traffic packets for the purpose of bridging the VoIP traffic between VoIP domains, Network Address Translation (NAT) and basic local VoIP server functions when IP connectivity to the WAN is lost.
- **TFTP Server:** Service providers use Trivial File Transfer Protocol (TFTP) servers to download configurations to the routers, and other systems such as IP phones.

3 In 1978, the International Standards Organization (ISO) introduced the ISO model for Open Systems Interconnect (OSI)

2. Description of the Future Networks Technology

The following network technologies will be described in the following subsections:

- Section 2.1 - PSTN/IN with migration to future networks
- Section 2.2 - 3G Wireless
- Section 2.3 - WiFi
- Section 2.4 - WiMAX
- Section 2.5 - Cable
- Section 2.6 - Internet Core
- Section 2.7 - General IP based technologies as basic to future networks

2.1. PSTN/IN to Future Networks Migration

2.1.1. Introduction

Many telecommunication service providers are actively planning to migrate to future networks. A large part of this migration will be the movement of traditional voice and data services from a PSTN network that uses IN signalling. In this paper, we will refer to these as PSTN/IN networks.

These PSTN/IN networks have been developed to the point where they are highly reliable, reasonably secure, and provide a large array of voice and some data services. Since these networks provide a "lifeline" to the outside world for many people, they are required to provide a number of public services. In addition, regulatory bodies seeking to foster competition have mandated a number of other capabilities, such as equal access and number portability. When large-scale migration of subscribers from PSTN/IN to future networks occurs, these capabilities must be provided unless significant regulatory changes are made.

This transformation is just beginning. While Voice over IP (VoIP) networks have been deployed in a number of places in Europe, they still represent a very small percentage (1% as of YE'05) of overall telecom subscribers[4]. VoIP is typically provided as a low- or no-cost option to consumers, sometimes as part of a service bundle. When large-scale migrations occur, as some carriers are currently contemplating, customers may be moved without their knowledge or consent. In this scenario, customers will certainly expect to get, at a minimum, the same functionality, reliability, and security as before.

Currently, the groups that are using VoIP tend to be competitors to the incumbent carriers (e.g., cable operators and Internet service providers). However, many mainstream providers are now considering or actively planning migration in order to attain the same cost structure and remain competitive. In addition, future networks hold out the promise of new revenue-generating services, and converged services that combine the best features of wireline, wireless, video and high-speed data networks.

The rollout is likely to occur gradually over a number of years. Even in 2019, over 30% of total main lines worldwide will remain Plain Old Telephone Service (POTS).[5] There is an extremely large embedded base of PSTN/IN equipment to be changed out. Besides the large capital investment required, the operational complexity of the actual migration is considerable. In addition, many technical and business-related issues are still to be resolved. For example, the interconnections between peer future networks, both technical and settlement arrangements, have yet to be fully defined. This results in most traffic that has to leave a carrier's future network being routed to the PSTN/IN, even if the destination network is also a future network.

In the next section we examine some Europe specific trends for PSTN/IN networks.

4 "Global VoIP Has Arrived; Just Not As Expected!" December 2005, In-Stat.

5 "Carrier NGN Migration Strategies Set VoIP Market Timing," April 2005, In-Stat

2.1.2. Usage and Market Trends

The traditional wireline narrowband phone market is not growing in Europe as a whole. In Western Europe there is actually negative growth in the narrowband access lines. The Western Europe Compound Annual Growth Rate (CAGR) is projected to be about –5% from 2005 to 2011 for narrowband access lines (see Figure 2). Eastern and Central Europe has slight projected growth at 1% CAGR of the wired narrowband. For entire Europe the projection is a –3% CAGR for narrowband access lines. The revenue from voice services to the service providers is also reflecting the reduced number of lines to collect revenues from and is projected at a CAGR of –5% (see Figure 3).

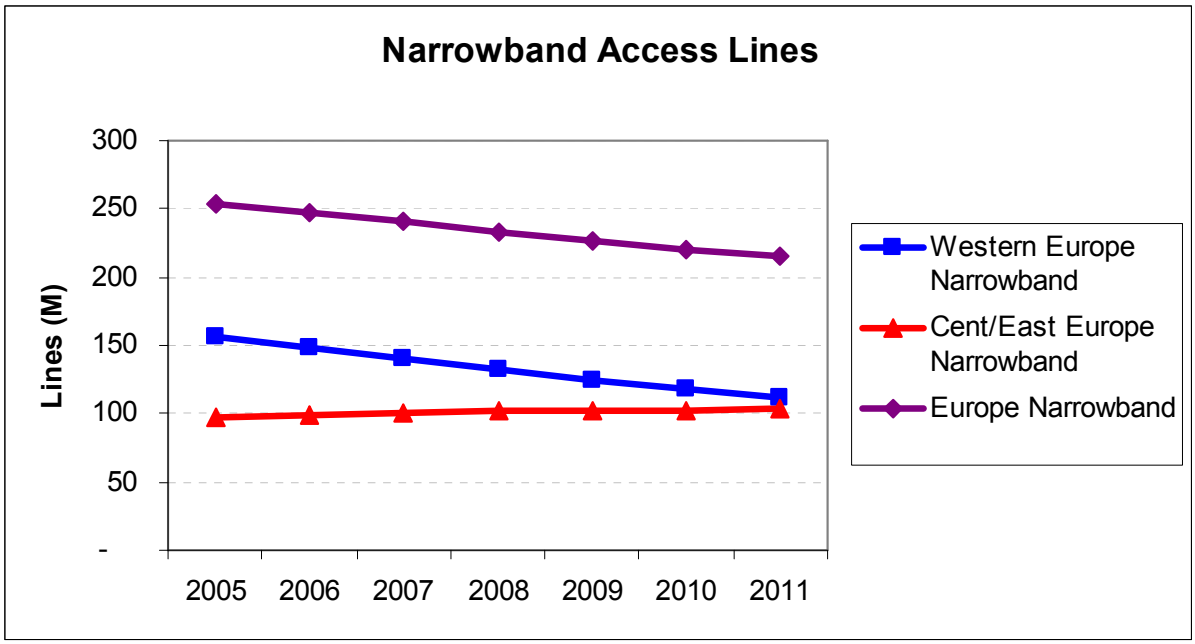


Figure 2: Projected Narrowband Access Lines [6,7]

6 "Western Europe Fixed Communications Demand," Pyramid Research, June 2006

7 "Central and Eastern Europe Fixed Communications Demand," Pyramid Research, June 2006

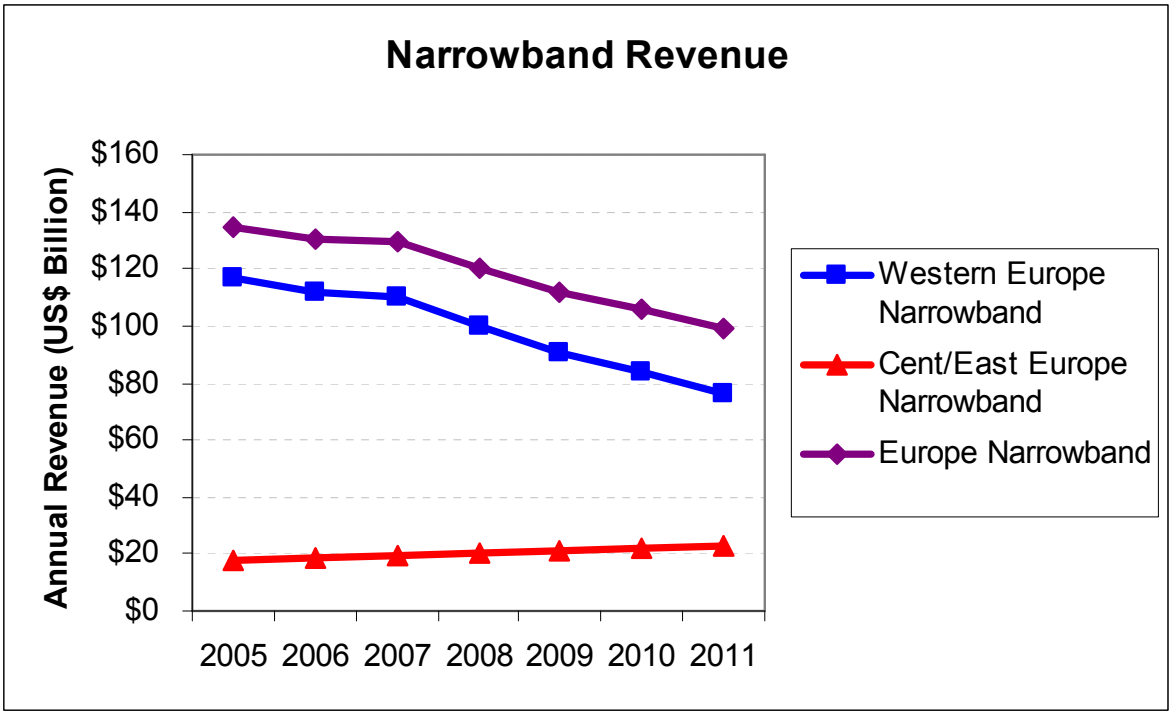


Figure 3: Narrowband Revenue Projections [5, 6]

There is growth in the broadband segment for service providers with growth in DSL, Fibre-To-The-Home or Curb (FTTH/FTTC), cable, broadband fixed wireless, satellite, etc. (see Figure 4 and Figure 5). Growth is significant but due to the competitive landscape of multiple service providers offering the service, there are pricing pressures that keep prices in check. The overall result is a decline in revenue projections for the European service providers. When combining revenues for both narrowband and broadband services the European CAGR is –1% between the years of 2005 and 2011 (see Figure 6).

What the above text shows, is that the service providers need to build out the new technology and define new services to maintain revenue growth and replace services in the declining market areas. Introducing new technologies also improves operational performance that reduce the over all cost to supply service. For data services the cost of service is usually quoted as the cost to provide the transfer of a Mega Byte (MB) of data across the network. The barriers to entry were the regulatory framework provided by each country and the cost of the equipment and interconnections to build the network. With new technologies some of these barriers are no longer in existence (e.g., when a service provider sells voice services over the Internet globally without having local equipment offices). These new service providers may not be covered by the regulatory guidelines that apply to the existing service providers. However, these service providers are part of the additional competitors who are creating pricing pressure in the marketplace.

The new competitive service providers will remain in business as long as they provide acceptable service levels to the subscriber base. Service level is not only availability and reliability but also correct billing, access to customer care and addition of new services.

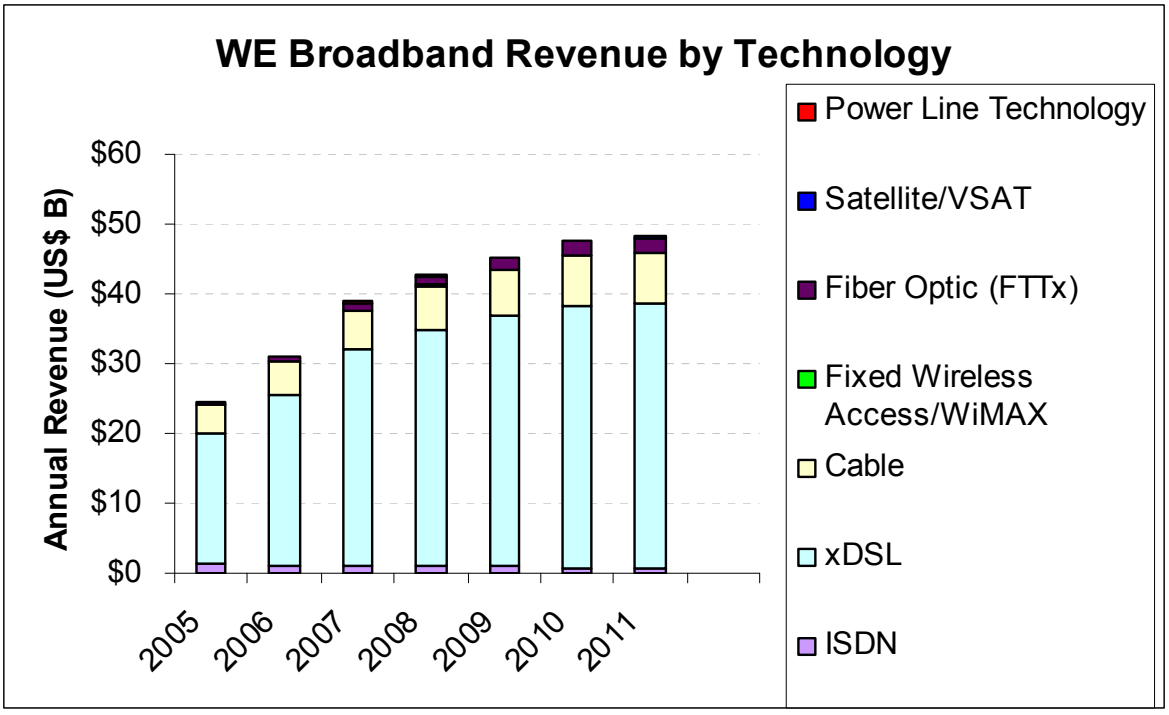


Figure 4: Western Europe Estimated Revenue by Technology [5,6]

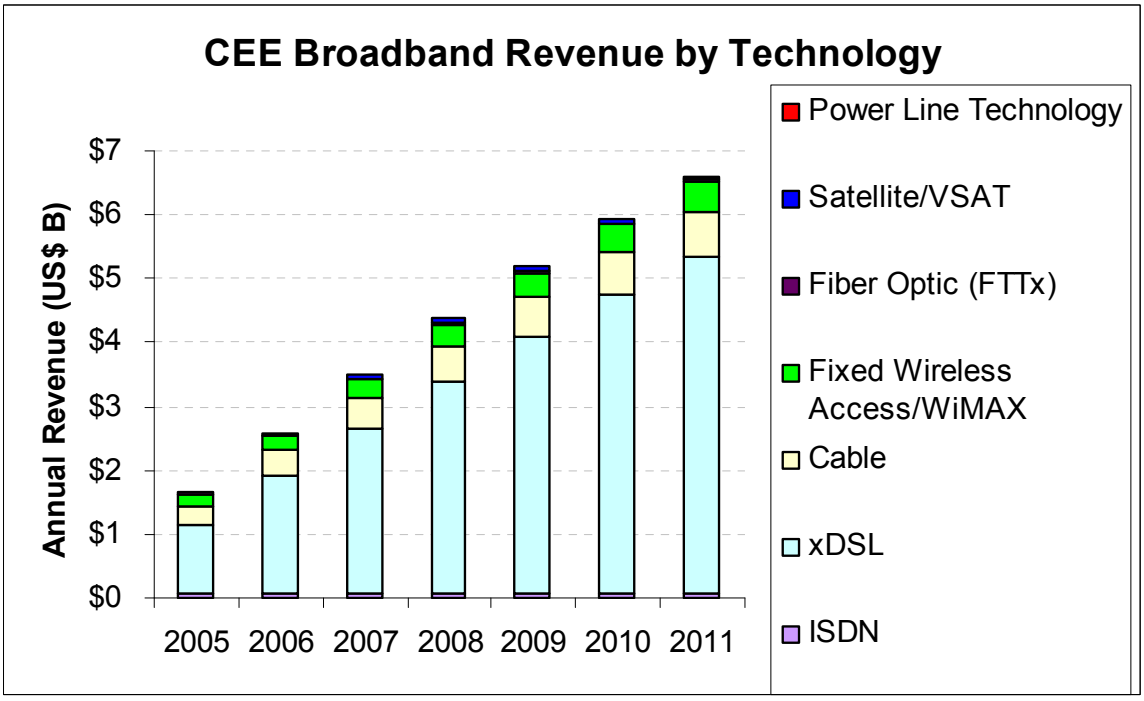


Figure 5: Central & Eastern Europe Estimated Revenue by Technology [5,6]

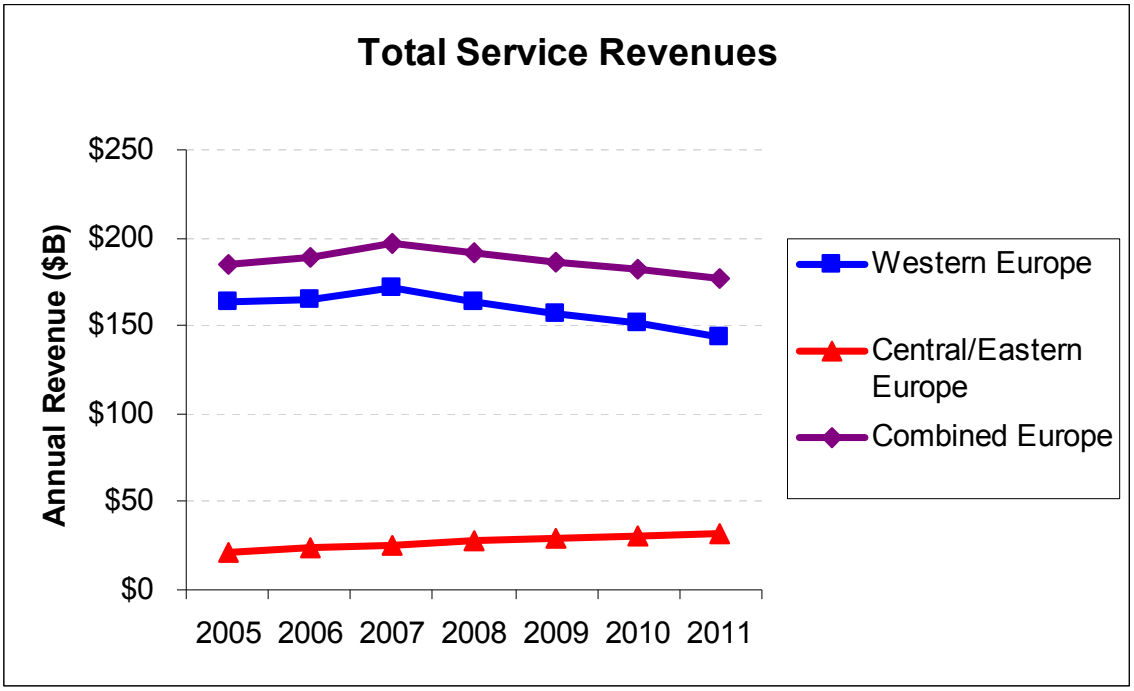


Figure 6: Estimated Services Revenue by Year [5, 6]

2.1.3. Architecture of PSTN/IN to Future Networks Interconnection and Migration

A depiction of the network architecture of the PSTN/IN to future Networks interconnection and migration can help clarify the interconnection points and how the networks will evolve over time. The interconnection of PSTN/IN and future networks is shown below (see Figure 7). In this figure, calls traversing the boundary between the two types of networks will interconnect at the transport plane through an MG, and at the control plane through a Signalling Gateway (SG).

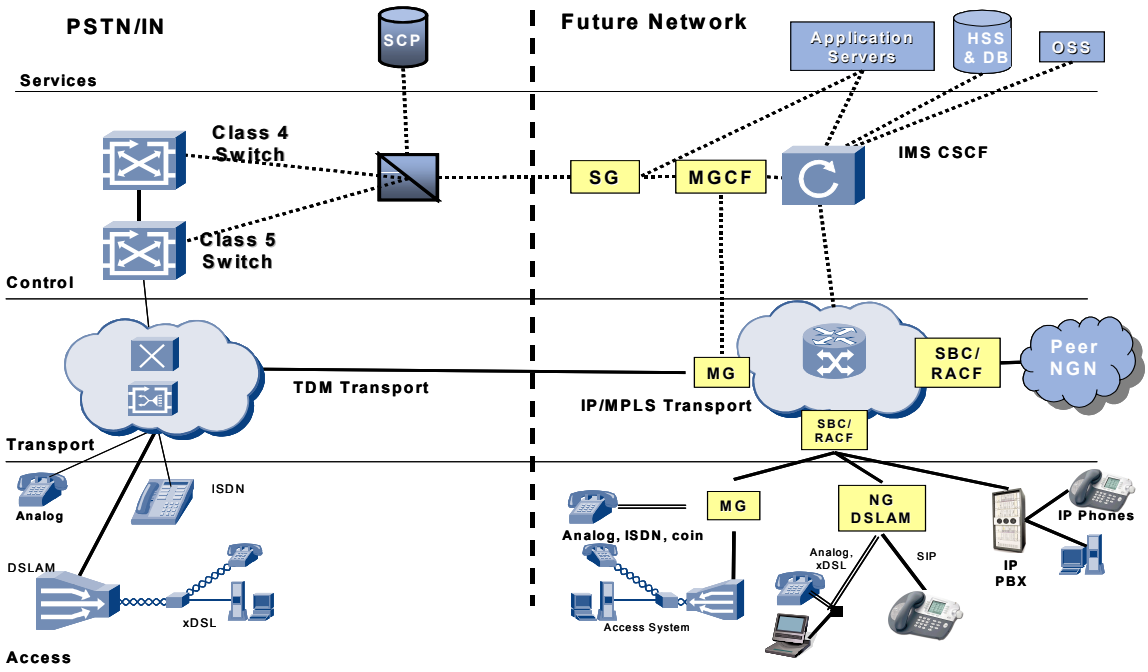


Figure 7: PSTN/IN and Future Networks Interconnection

A carrier may use one of several migration strategies to move existing PSTN/IN customers onto a future network (see Figure 8). These strategies include:

- Some users will opt to move to Session Initiation Protocol (SIP) and IP endpoints in order to take advantage of advanced features offered over IP. These users will need to acquire new user equipment (e.g., handsets, desk sets, or softphone). They will also require a broadband connection to the network.

- Users who opt to keep their legacy equipment (PSTN/IN or IP) can have their lines moved to a Next Generation DSLAM (NG-DSLAM) that offers interconnection to PSTN, and IP lines, with a SIP or H.248 interface to the network. These NG-DSLAMs will provide features that will allow complete PSTN/IN emulation to the end user (i.e. they will make the user experience identical to the current PSTN/IN).

- Carriers can decide to move blocks of PSTN/IN users and their existing Digital Loop Carriers (DLCs) onto the future network by interfacing the DLC via an access MG. The MG will convert the Time Division Multiplexed (TDM) bearer to IP and SIP signalling.

- Some lines may continue to be homed on the PSTN/IN in order to access services that are not available or economical to duplicate on the future. It is possible that the transport backbone between the TDM switches will be converted to IP, but this will be transparent to the user. For this reason, the PSTN/IN and the future networks may have to coexist for an extended period

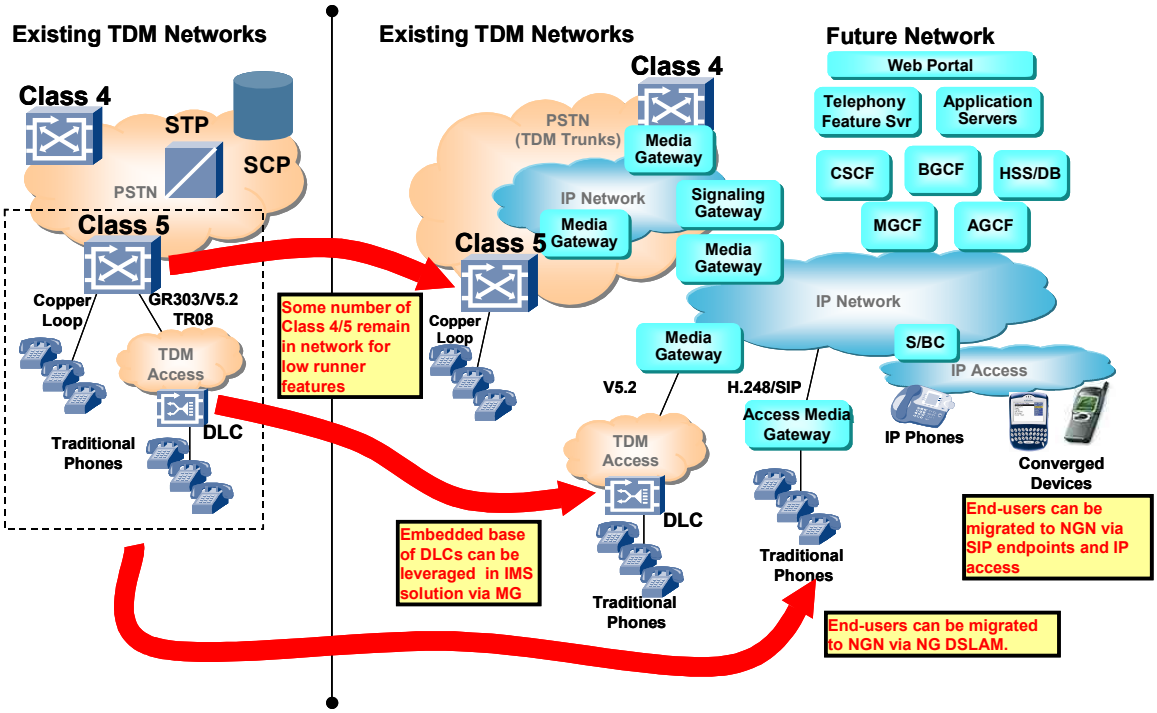


Figure 8: Migration of PSTN/IN customers to Future Network

2.1.4. Major Components of a Future Network

To interconnect PSTN/IN networks and customers to future networks, some new technology network elements are required. A number of these elements, common to several in-scope technologies, are described in Section 1.1. The following descriptions cover additional network elements that are common in the PSTN/IN to future networks architecture.

- **AGCF:** The Access Gateway Control Function (AGCF) controls one or more Access Media Gateways to which PSTN/IN users are connected. It handles registration, authentication, and security for the user. It also can provide emulation of PSTN/IN tones and behaviour so that the user experience does not change.

- **AMG:** The Access Media Gateway (AMG) provides inter-working between the packet-based transport used in the future network and lines from the circuit-switched network. It is under the control of the AGCF.

- **SG:** The Signalling Gateway (SG) is responsible for signalling transport inter-working between the future network and existing networks such as PSTN/IN.

2.1.5. Brief Description of the Underlying Technology

The standards for inter-working between PSTN/IN and the future network are being developed under the oversight of the ITU. Significant amounts of work are being done in the ETSI TISPAN working groups, which then contribute their work to ITU.

The signalling protocols for PSTN/IN that have been defined and are under the control of the ITU, include Signalling System #7 (also known as SS7 or C7). Some of the different protocols include ISDN-User Part (ISUP) basic transport, call control messages, and the Message Transport Part (MTP). Alternatively, the Bearer Independent Call Control (BICC) protocol may be used. For application signalling, the Intelligent Network Application Part (INAP) provides the application layer protocol, while the Transaction Capabilities Application Part (TCAP) and Signalling Connection Control Part (SCCP) provide supporting querying and routing capabilities. On the access side, analogue signalling schemes or Q.931 and Q.932 for ISDN terminals are used.

The signalling protocols for future network are primarily based on IP, and are developed under the oversight of IETF. They include SIP, which is used to set up and tear down sessions (or calls); H.248, which is used to control media gateways; H.323, which is used to control legacy IP telephones; and Hypertext Transfer Protocol (HTTP), which is used to interact with web-based applications.

The inter-working for these protocols is largely defined at the functional level; however, the details of implementation are still being worked out.

2.1.6. Characteristics Regarding Network Technology

There are a number of considerations related to PSTN/IN to future network interconnection and migration. These are categorised in the following list and described more fully in the following subsection.

- Voice Traffic
- Signalling Traffic
- Access
- Applications
- Data Services
- Operations, Administration, Maintenance & Provisioning (OAM&P)

2.1.6.1. Voice Traffic

Future network technology is expected to be lower cost since it is based on technology used for the Internet. In addition, current regulations for provision of voice services over Internet technologies tend to be less stringent, further lowering the cost to providers. These lower barriers to entry may result in many smaller voice providers, some of whom may have little or no experience in providing voice services. Also, the equipment they purchase may not meet the levels of quality, reliability, and security of the PSTN/IN equipment. While the equipment costs are lower, the equipment may be unable to provide all the functions required in some Member States. This limits the service provider to those Member States having less stringent requirements.

Even the incumbent carriers who deploy an overlay future network, or convert their existing networks, may face some of the same problems due to immaturity of some of the standards, equipment, and business arrangements for interconnection. The migration from PSTN/IN to future networks in the European Union (EU) will involve a large number of ISDN Basic Rate Interface (BRI) and ISDN PRI that have to be migrated and emulated. These issues are described in more detail below.

Security:
Several new types of network elements that function as gateways are being deployed. Since they are based on Internet technology, they can be vulnerable to external (i.e. hacker) or internal (i.e. malicious employee) attacks. Gateways are particularly vulnerable to external threats.

Appropriate security standards (e.g., ISO/IEC 18028 and X.805) should be followed, and regular security assessments should be conducted. The following items must be ensured:

- All network gateways such as MGs and Session Border Controllers (SBCs) must be highly secure and must protect the future network from internal and external attacks. In addition, it should not be possible to launch an attack into the PSTN/IN from these gateways.
- Bearer traffic confidentiality must be maintained end-to-end.
- Data integrity should be maintained so that corruption of bearer traffic stream can be easily detected.
- Communication security should be maintained to prevent the insertion of unauthorised or malicious packets into the bearer traffic stream.

Network and Traffic Management:
Due to the completely different technology used, future networks will require new traffic engineering Methods and Procedures (M&Ps) and tools. Accurate traffic engineering is required in order to allow network growth that balances investments with revenue, and to avoid traffic congestion and consequent degradation of service.

Many different types of traffic will be mixed in future network: voice, data, video, signalling, with different QoS requirements. Most carriers do not have experience with managing a network with all of these types of traffic intermixed. Mixed traffic presents new challenges in terms of contention for network resources, and the complexity of engineering appropriate amounts of capacity for multiple services with very different traffic profiles and busy hours.
This requires further study with the aim of developing monitoring and management tools that will facilitate the operations and management of future networks.

As future networks are introduced, existing PSTN/IN traffic will increasingly have to be re-routed from their existing paths to future network gateways. This will create new traffic patterns, and possible congestion points in the PSTN/IN. Also, the amount of traffic through the gateways will vary over time, peaking when roughly half of the traffic is on the future network, and then declining as the PSTN/IN declines. Traffic engineering studies in these networks should be conducted before moving large amounts of traffic to future networks.

PSTN/IN network management controls don't extend into future network, and future network controls are not fully defined and verified. For example, mass-calling events such as radio or television call-in events may cause focused overloads, or natural disasters may cause more widespread congestion. Related standards work is in progress and should be implemented.

Without adequate controls, calls can be established which exceed overall bandwidth resulting in lost packets and lower QoS. Standards work on these items, such as the work on the Resource and Admission Control Function (RACF) must be completed and recently completed work[8,9] should be implemented.

Routing and Interconnection:
Calls will increasingly cross multiple networks with different technology as future networks are deployed. The end-to-end reliability and quality of voice calls must be maintained in this new environment. Objectives and standards-based requirements on new technologies are being developed. Carriers must consider end-to-end reliability and QoS within future network, to peer future network, to PSTN/IN, and to access networks. Multiple interconnection points with re-routing on failure are needed.

Multiple codec conversions are possible on calls traversing several networks, including both PSTN/IN and future network, leading to voice quality degradation. Procedures should be developed that limit the number of codec conversions on a call. Interconnection issues between peer future networks should be resolved to minimise the need for such conversions.

The interconnection of peer future networks via SBC or RACF functions is being standardised. There are likely to be different vendor packaging of SBC and RACF functions, to be reconciled in network implementations and adherence to routine integration and regression testing to ensure future network reliability and security.

Transport:
Some future networks will replace highly reliable Synchronous Digital Hierarchy (SDH) transport with MPLS and Ethernet. Scalability, reliability, and OAM&P in the Wide Area Network (WAN) should be looked at, as well as addressing, forwarding, and inter-working before large-scale deployments are possible.

Variation in QoS in future networks could result for PSTN/IN users when calling future networks and the PSTN/IN carrier may experience more customer complaints. All voice carriers should implement the previously mentioned strategies to ensure QoS.

2.1.6.2. Signalling Traffic

Signalling for call control is an area of high vulnerability for both PSTN/IN networks and future networks. This is because failures or deliberate sabotage of the signalling network can have severe consequences, up to and including the blocking of all calls on the network. PSTN/IN signalling has been relatively secure because the signalling traffic is segregated onto separate physical links, and the interconnections are made between “trusted” networks (i.e. large service providers). This will no longer be true in the future network environment and will result in security and reliability risks to both the PSTN/IN and future networks.

PSTN/IN signalling was designed around the assumption that other interconnecting networks can be trusted in terms of security and quality. As mentioned earlier, lower barrier to entry for

8 ETSI/TISPAN Resource and Admission Control Sub-system (RACS); Functional Architecture, June 2006.

9 ITU-Recommendation Y.2111 (formerly Y.RACF), Resource and Admission Control Functions in Next Generation Networks, October 2006.

future voice service providers may result in many new future entrants to whose networks the PSTN/IN carriers will interconnect, and whose networks may not be as reliable or secure. Increased security measures (e.g., monitoring, filtering) in PSTN/IN networks may be needed to protect against corrupted signalling messages originating in future networks. In addition, the following precautions should be taken in the future network:

- Design SG security to ensure high availability.
- Implement IDS and stateful rate limiting firewalls to reduce the impact of Denial of Service (DoS) attacks.
- Use Firewalls, filters, and ACLs to maintain separation of IP and C7 interfaces.
- Restrict access to applications and configurations by designing privilege levels and implementing Role Based Access Control (RBAC).
- Implement data confidentiality, communication security and integrity measures between IP SG and C7 elements.
- Ensure that future network users do not have visibility into future network topology and addresses.

In the PSTN/IN, signalling control traffic is physically separated from bearer traffic, but in future networks it is not. Therefore, signalling messages in future network are more vulnerable to corruption (deliberate or otherwise), and may be more subject to congestion due to bearer traffic overload on common links and nodes. Stringent security controls must be implemented in future networks to prevent attacks, especially at gateway elements. Also, adequate capacity management and call admission control processes are required to prevent traffic overload.

Signalling traffic to and from the PSTN/IN goes through SG and MGCF, which are new elements that will carry a high volume of calls. They must meet very stringent reliability requirements. Universally accepted reliability requirements are not available for service and applications supported by future networks. End-to-end reliability studies will determine appropriate requirements. The SG and MGCF must have high nodal availability with physical and geographic diversity of node and link. Multiple interconnection points are required which are engineered to handle entire load in case of node or link failure with re-routing and short switchover times.

As PSTN/IN signalling points are retired, the signalling traffic will have to be re-homed to SGs, exposing the network to vulnerability due to procedural errors during transition. Careful engineering and coordination is needed for signalling traffic movements between PSTN/IN and future network (see Figure 9).

There are a number of signalling protocols inter-working areas to consider:

- National and regional variations on standards.
- Inter-working of future network protocols with various implementations of ISDN protocols. When the Q.931 and Q.932 ISDN terminal protocol standards were developed, they allowed flexibility in implementation. Also, different national regional bodies allowed further enhancements and variations resulting in a wide variety of national implementations. In Europe, ISDN phones were fairly widely deployed (much more so than in the US). So any new networking method should be backward compatible with the ISDN phones.

Call looping and excessive hops leading to excessive delay are possible on calls between PSTN/IN and future network, until appropriate signalling inter-working procedures are finalised.

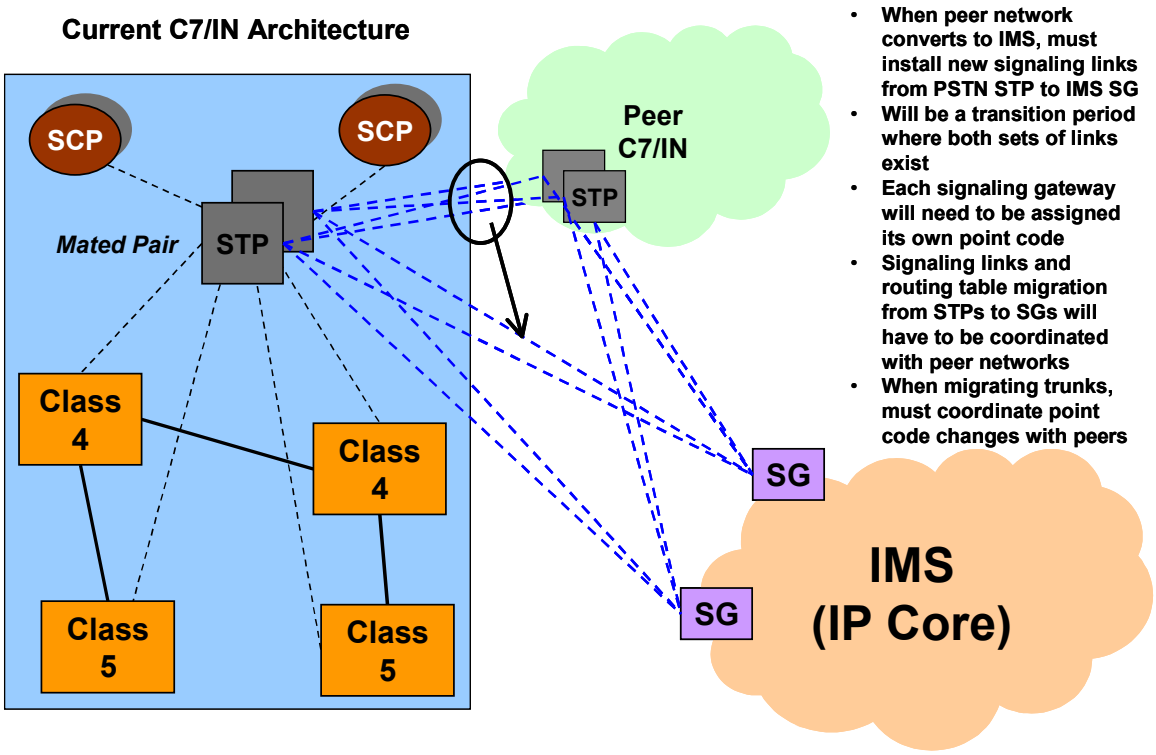


Figure 9: PSTN/IN Signalling Link Interconnection to Future Network

2.1.6.3. Future Network Access

Access networks will undergo considerable changes. As the sheer volume of access lines is extremely large, the vulnerability to equipment problems and human error is considerable. However, problems will usually be localised.

More access equipment may be located outside controlled Central Office (CO) environment due to the carriers' desires to close local switching offices. This equipment may then be:

- More vulnerable to sabotage
- Requiring longer to be repaired after failure
- Lacking in backup power supplies

Carriers must provide access designs, which meet stringent reliability and security requirements (e.g., for lifeline services).

The core network must be protected against IP endpoints that could be used to attack the network. They should not be allowed to see the core network topology and addresses. An SBC or an RACF function is needed to protect the network at all access interconnection points.

Physical location of subscriber lines is more difficult to determine for emergency services due to the portability of SIP wireline terminals. Carrier must have an accurate method of keeping track of users physical location for emergency services.

2.1.6.4. PSTN/IN Applications on Future Networks

Customers who move or are moved onto a future network will expect to get the same or similar application functionality as they had with the PSTN/IN. Customers who stay on the PSTN/IN will also expect applications to have same functionality and quality (emulation) when it crosses the boundary between the PSTN/IN and a future network. Standards are being developed for inter-working some common applications in order to provide either:

- Service emulation: same functionality and method of user operation
- Service simulation: equivalent functionality, though operation may differ.

See Figure 10 for a view of PSTN/IN application inter-working with future network.

There are many other applications that are carrier or region specific or have unique implementations and are just beginning to be addressed in standards (e.g., IN-based, operator services, routing features, call centres, mass calling, emergency, and messaging). Significant effort will be required to migrate or retire all of these services. These applications will have to be considered on a case-by-case basis. This may slow down the rate of migration to future network.

Future network mass calling and auto dialler could flood the PSTN/IN gateways unless appropriate procedures are adopted. Both inbound and outbound services to and from future network would be affected. Standards work on these items must be completed and implemented.

PSTN/IN business users may have developed customer applications that rely on the PSTN/IN data (e.g., customer Information Technology (IT) systems that take output of PBX call data). These applications may require changes when moved to future network. These applications may have to be redeveloped or changed, which may be a disincentive for some enterprises to move to future network.

Allowing future network to access IN applications may open IN to security vulnerabilities and malfunctions of future network. See signalling traffic discussion above.

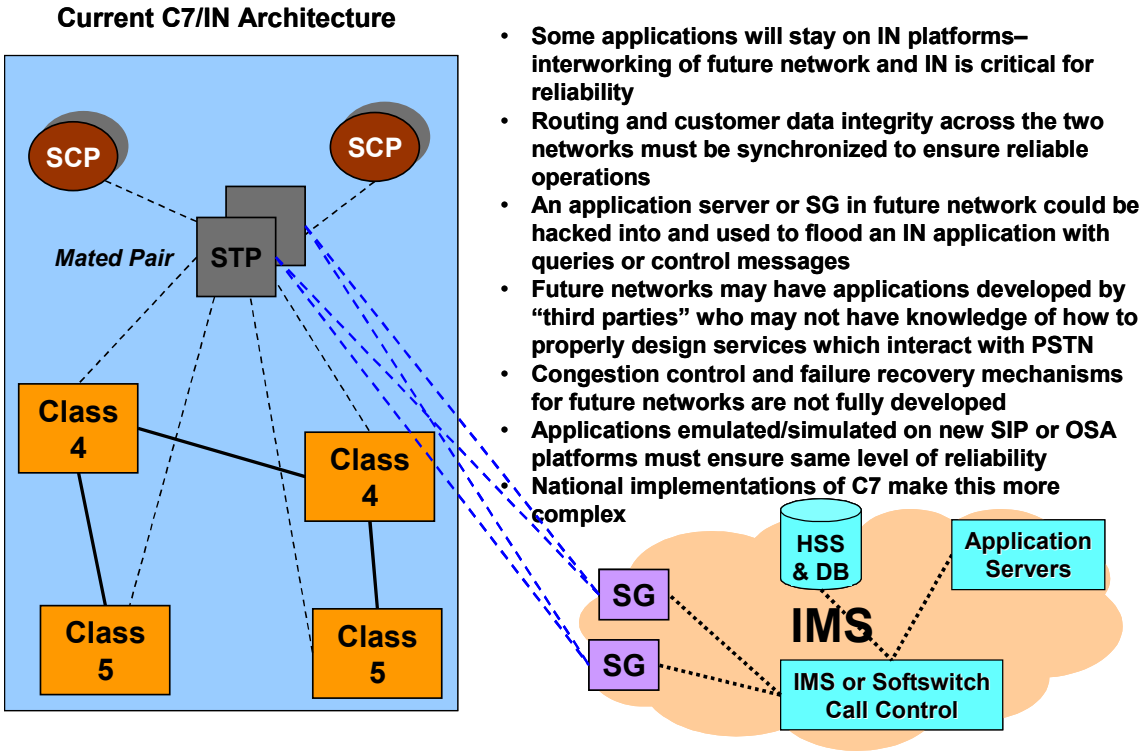


Figure 10: Application Migration

2.1.6.5. Data Services

While the PSTN/IN handle primarily voice traffic, there are a number of data services that are provided over their infrastructure. Low speed data services are used by many small businesses for applications such as "point of sale" terminals and Automatic Teller Machines. SDH leased lines are used by larger businesses and often carry mission-critical traffic.

Emulation of some PSTN/IN data services are being to be defined for offers within the future network, or across the PSTN/IN and future network boundary. The following are examples of such services:

- Low speed data services (e.g., the many implementations of X.25)
- ISDN concatenated channels (n x 64kbps)
- Private lines

Until this functionality is provided via future network, these users will have a disincentive to move their lines, since it will require new customer premise equipment.

PSTN/IN business users may currently subscribe to highly reliable private line services with multiple homing in order to protect their mission critical traffic. They may be wary of moving sensitive traffic to future network until its reliability and security have been proven. Data should be collected on reliability and security in order to address problems and reassure business customers. SDH-based transport services that require high reliability will need to be converted if SDH is phased out. Equivalent end-to-end reliability must be maintained in the new transport network (e.g., Ethernet and MPLS).

2.1.6.6. OAM&P in Future Networks

One of the promised benefits on future network is reduced operational cost. This is due to a number of factors, such as eliminating the need for multiple special-purpose networks, and using newer technologies that are easier to operate and maintain. However, the complexity of future networks presents its own challenges that must be managed (see Figure 11).

There will be a need to operate and manage increased network complexity in several dimensions at the same time, such as:

- Multi-technology, multi-vendor, Inter-network connections and convergence
- Multi-service provider (application service providers, content providers, carriers, enterprises) or multi-location (regions) interfaces and interactions
- Multi-media, multi-services management as an integral part of network operations
- End-to-end service security, availability, QoS and SLAs

There is a desire to improve several business performance dimensions at the same time:

- Reduce operations costs and keep them low
- Evolve network infrastructures to future network without interrupting current service delivery
- Operate & manage a continuous influx of new services from new providers
- Manage multi-media service applications and customer self management as an integral part of operations
- Maintain high levels of customer satisfaction through speedy and flawless service delivery performance

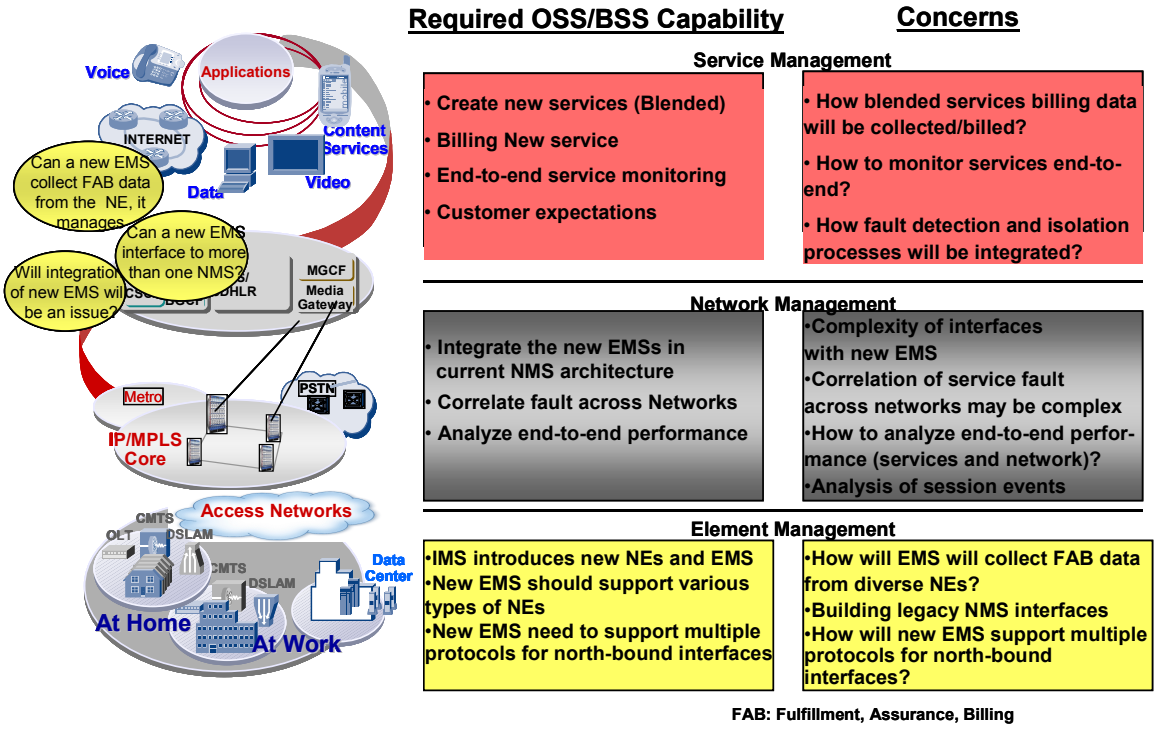


Figure 11: OAM&P in Future Networks

Many new M&Ps and Operations Support Systems (OSS) and Business Support Systems (BSS) will need to be developed and deployed, such as:

- M&Ps & OSS and BSS for End-End Service Fulfilment, Assurance & Billing
- M&Ps & OSS and BSS for Services & Network Planning and Engineering Capability Delivery
- M&Ps for electronically Enabled (e-Enabled) Inter-Carrier agreement administration
- M&Ps for e-Enabled supplier, partner (and customer) agreement administration

Carriers will need new Security Policies & Management for:

- Network & network services
- Operations infrastructure and security administrators
- Inter-carrier connections, contracts and oversight

The procedures for Disaster Recovery and Business Continuity Policies, Plans & Management will need to be reworked, both internal and for Inter-network or Inter-carrier.

Tariffs and charging on inter-network calls may require changes due to loss of geographic association of endpoints. Carriers will have to re-work their tariff and charging structures as appropriate. The chart below provides an overview of some of the costs and anticipated operational benefits of migration to future network (see Figure 12).

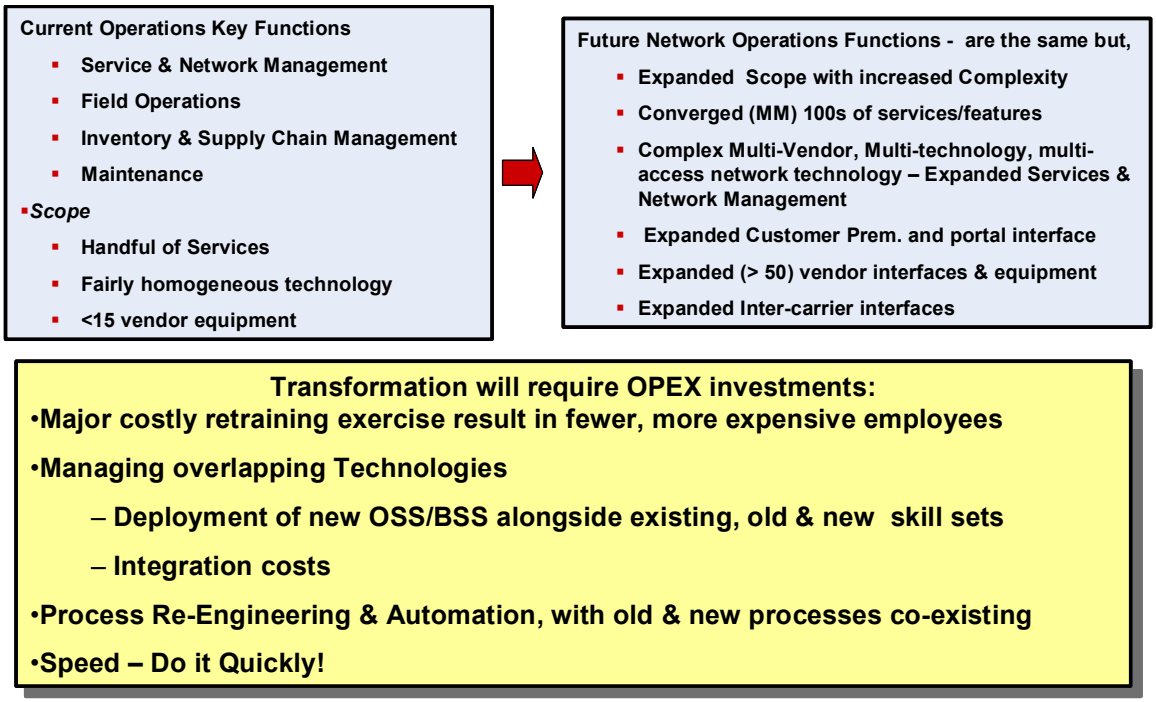


Figure 12: OAM&P in Future Networks

2.2. 3G Wireless Networks

2.2.1. Introduction

Universal Mobile Telecommunication Service (UMTS) also known as Wideband Code Division Multiple Access (WCDMA) is the primary choice of 3G wireless technology in Europe. Driven by European Telecommunication Standards Institute's (ETSI) 3rd Generation Partnership Project (3GPP) standards organisation, UMTS has already been deployed in much of Europe for field trials and commercial deployments are happening right now. UMTS networks are expected to coexist with 2G Global System for Mobile Communication (GSM), General Packet Radio Service (GPRS), and Enhanced Datarate for GPRS Evolution (EDGE) networks for the next several years. GSM networks are currently very widely deployed in Europe, with coverage reaching a vast majority of the population. Since coverage of UMTS networks will initially be in densely populated areas, it is expected that in its early adaptation, UMTS subscribers will be handed off to GSM networks as they roam out of UMTS coverage.

Most major service providers in Europe have adopted UMTS as the technology of choice for high-speed data services. Even though deployment started at a very slow pace due to monetary and initial technological constraints, adaptation has accelerated with several commercial launches being announced in the past few months.

Current deployment of UMTS is primarily for Rel99[10] and Rel4[11] architectures, which support both circuit and packet-based services and depend on ATM in the Radio Access Network and ATM or Internet Protocol (IP) in the core network. Rel5[12] networks with IMS core are on trial in many operators' networks. IMS is a packet-based technology with full IP-based implementation in the core network. With Rel6[13], IP will also be implemented in the radio access network.

In eastern and northern Europe, North American 3GPP2 standards-based Code Division Multiple Access Evolution Data Optimized (CDMA 1X EVDO) is also being deployed. EVDO is fully compliant with International Mobile Telecommunication (IMT) - 2000 definition of 3G wireless. However, its deployment in Europe is expected to be fairly limited due to limited availability and high cost of dual mode handsets and data cards that support GSM and UMTS and CDMA EVDO.

The move to 3G wireless is primarily driven by the need to provide high-speed data services (up to 2 Mega bits per second (Mbps) per user) to end users. The underlying technology also enables voice services at a lower cost, though it will be a while before UMTS is the technology of choice for voice only services; the embedded base of GSM is expected to handle circuit voice services until the end of its life cycle. However, the primary mobile technology for accessing the Internet as well as other IP-based services will be provided by UMTS.

10 3G TS 23.002 V3.6.0 (2002-09)

11 3GPP TS 23.002 V4.8.0 (2003-06)

12 3GPP TS 23.002 V5.12.0 (2003-09)

13 3GPP TS 23.002 V6.10.0 (2005-12)

2.2.2. Usage and Market Trends

After a fast growing period since the early 90's, the overall Western European wireless market is approaching saturation. The overall wireless penetration rate is forecasted to reach 81% of the total population by year-end 2006 and is expected to stay flat around 83% by the end of 2014[14]. The total Western European wireless market generated about € 140 billion in 2005.

As the subscribers migrate from the current GSM to UMTS networks, the mobile data business is expected to grow from 17% in 2005 to 26% in 2010 as a share of the total wireless services revenue[15]. 3G migration is speeding up[16] as UMTS deployment had been widely rolled out despite a slow start. With the increasing use of the wireless data cards and the availability of the dual-mode (GSM and UMTS) handsets[17], Mobile Network Operators (MNO, a.k.a., wireless service providers) are moving more aggressively towards their UMTS networks deployment. 3G subscribers number will grow to 52 million, representing 16.3% of all wireless users, at the end of 2006 and is expected to grow to 246 million, equivalent to two thirds of all users, by the end of 2010. (i.e. CAGR of 47.5% over the 2006-2010 period.) With the decreases in per minute revenue of voice service (attributable to competitive market pressure, and national and supranational level regulatory intervention[18] MNOs will need to place a greater focus on driving revenues through usage from the mobile data and content services beyond the current basic SMS services.

Mobile Virtual Network Operators (MVNOs)[19] are currently playing a significant role in many western European countries and will continue to pose a threat to the MNO, as the regulators are instituting more competitive environment such as reduced call termination charges. MVNOs are expected to capture double digits market share (though lower figure in total revenue share) by year 2009 in the western European wireless market (see Figure 13[20]).

14 Strategy Analytics,, W. European Cellular User Forecasts, 2005-2010, Jan. 2006.

15 Yankee Group, 3G's Role in an Increasingly Competitive Wireless Marketplace, June 2006.

16 EU regulators (both national and supranational) specify 3G licensing conditions including coverage mandates and build-out time frames.

17 The initial high price of UMTS/GSM dual-mode handsets was part of the hurdle in UMTS growth in the early stage.

18 In December 2005, the two largest German MNOs (Vodafone and T-Mobile) came down from 0.132 to 0.11 Euro per min while E-Plus and O2 came down from 0.149 to 0.124 Euro per min for mobile termination charges. In additional to this voluntary reduction, the German regulator Bundesnetzagentur in June 2006 issued a statement in which it expressed its intention to further regulate mobile termination rates based on the costs of efficient service provision.

19 Mobile Virtual Network Operators, MVNOs, are resellers of the MNOs' services with low fixed-cost (little to no infrastructures to build) and higher variable costs (fees paid to the MNOs to access their networks). Compared to MNOs' business model, traditional MVNOs' business model yields lower margins by offering subscribers lower-priced services.

20 Yankee Group, 3G's Role in an Increasingly Competitive Wireless Marketplace, June 2006.

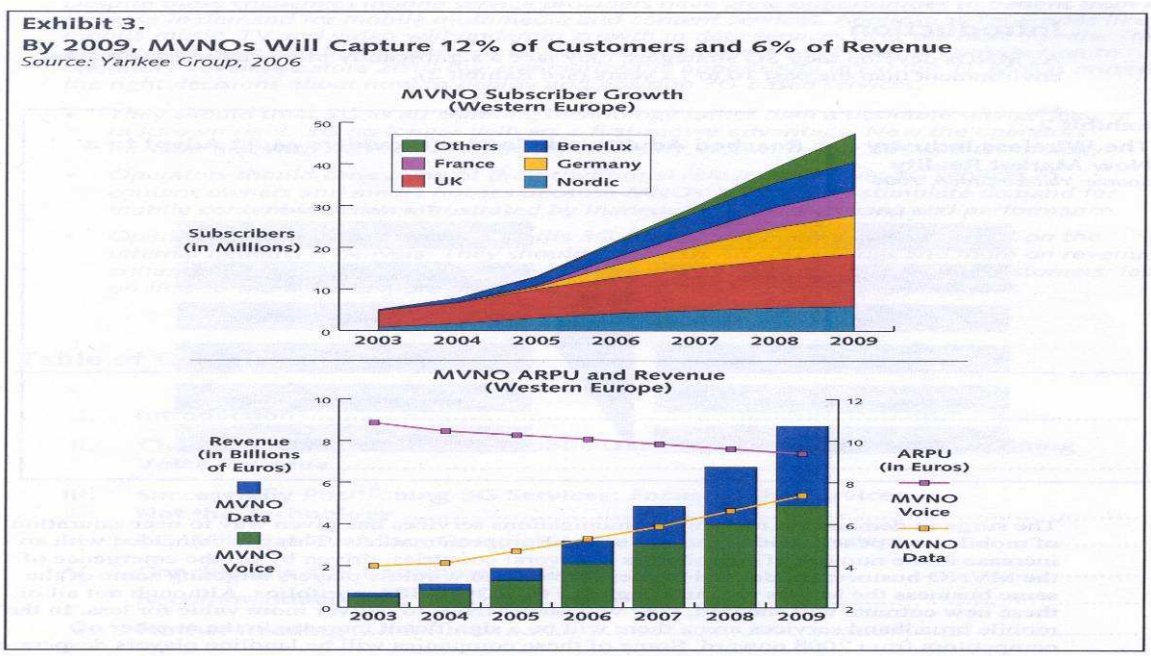


Figure 13: MVNO Growth Trends

2.2.3. Challenge of Complexity

Service providers need to communicate the benefits of 3G networks to their customers in terms of desirable new services applications, better coverage, and perceived lower pricing relative to value. It is imperative to create desirable mobile applications to drive successful adoption of 3G services. At the same time, service providers have to face the challenges associated with managing such a diverse set of services as more and more applications are being added to the services portfolio.

Interoperability across different networks (e.g., GSM, GPRS, and UMTS) could also be a concern for MNO since customers might expect these new service-offers to work across different network platforms in a similar matter.

For the most part, network service providers have been marketing the content to the consumers themselves. However, this approach is ineffective because of limited resources and expertise that MNOs can provide. Allowing the 3rd party content providers to actively sell their services to the end users directly will provide more channels other than only through mobile portals. Increased sales will help drive up the usage that 3G is capable of delivering. This will also stimulate more offerings and thus competition in the content provider domain.

Additionally, the increased complexity associated with successful and profitable 3G network operations should afford opportunities for vendors with managed services expertise.

2.2.4. Challenge of Competition

Increased competition in Western Europe has resulted in lowered Average EBITDA[21] Margin Per User (AMPUs), which has been falling since mid- 2004 and recorded a 7% fall in Q3 2005[22]. However, the Average Revenue per User (ARPU) is currently holding flat thanks to the increased per-user usage. Direct competition has come from new entrants (e.g., Hutchison), MVNO and reseller activities.

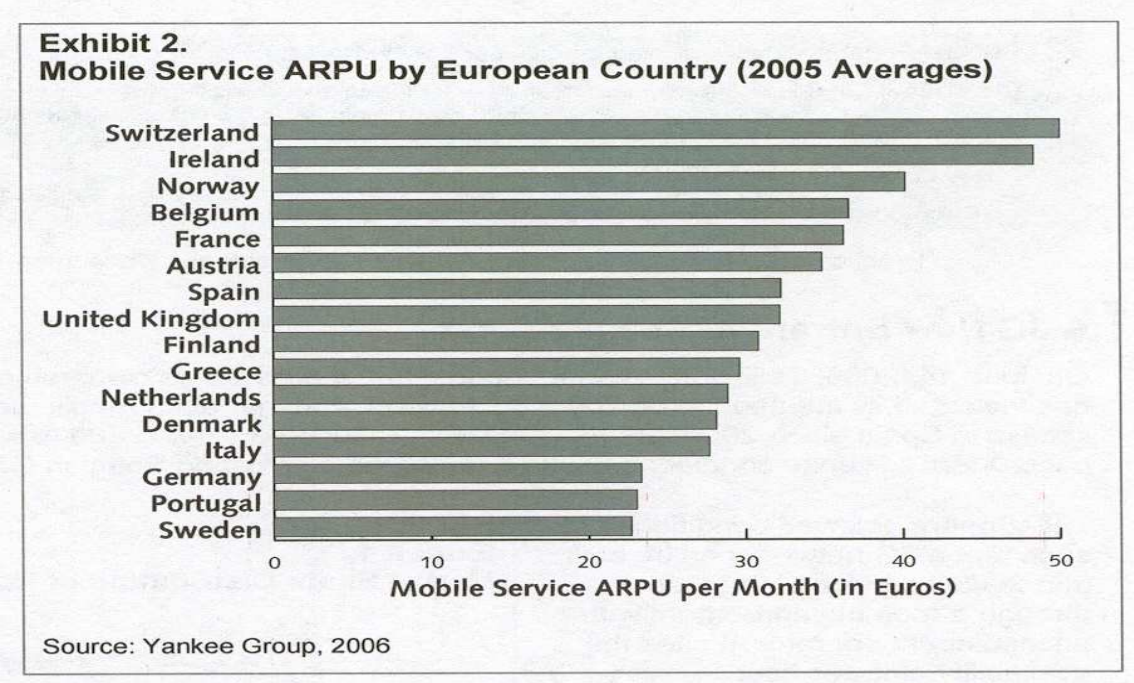


Figure 14: Mobile Service ARPU[23]

The availability of alternate access technologies, such as, Wireless Fidelity (WiFi), Mobile Worldwide Interoperability for Microwave Access (WiMAX) and Flash-Orthogonal Frequency Division Multiplexing (Flash-OFDM), poses a potential threat to the MNOs. There is also a slow but unstoppable demand toward integration of wireless and wireline communications in the home and office environment. WiFi provides a way that wireline operators can use to achieve Fixed Mobile Convergence (FMC) strategies. Partnering with WiFi service providers would allow MNOs to retain a share of home- and office-originated voice and data traffic[24].

21 Earnings Before Interest, Taxes, Depreciation and Amortisation

22 Strategy Analytics, Wireless Operation Outlook 2006, Jan 2006.

23 Yankee Group, Xfera Can Succeed in Spain with the Right 3G Strategy, Aug 30th, 2006.

24 Yankee Group, How Big Is Threat of Disruptive IP-Based Wireless Technologies to Mobile Operators? March 2006.

2.2.5. Architectures for 3G Networks

The network infrastructure for managed IP services is fundamentally the same, whether the access technology is UMTS or CDMA (see Figure 15). At the top is the Application Layer, comprising of various SIP, Parlay[25] and other application services belonging to the service providers as well as traditional web services accessible through the Internet.

Next to the Application Layer is the Session and Call Control Layer, consisting primarily of Call State Control Function (CSCF), Service Capability Interaction Manager, Media Resource Function Control (MRFC), Breakout Gateway Control Function (BGCF), Media Gateway Control Function (MGCF) and Policy Decision Function (PDF). The Home Subscriber Server (HSS) also belongs to this layer.

The core Transport Layer network is comprised of the Media Server, Media Gateway, Border Gateway as well as the Gateway GPRS Serving Node (GGSN) or Packet Data Serving Node (PDSN).

The Access Layer network consists of the 3G Mobile services Switching Center (MSC) as well as other components, which will be described separately for the sake of clarity.

The Endpoint Layer consists of various end-user devices, including mobile handsets, Personal Digital Assistants (PDAs), and wireless data-card enabled laptops. In future networks, these will act as SIP endpoints.

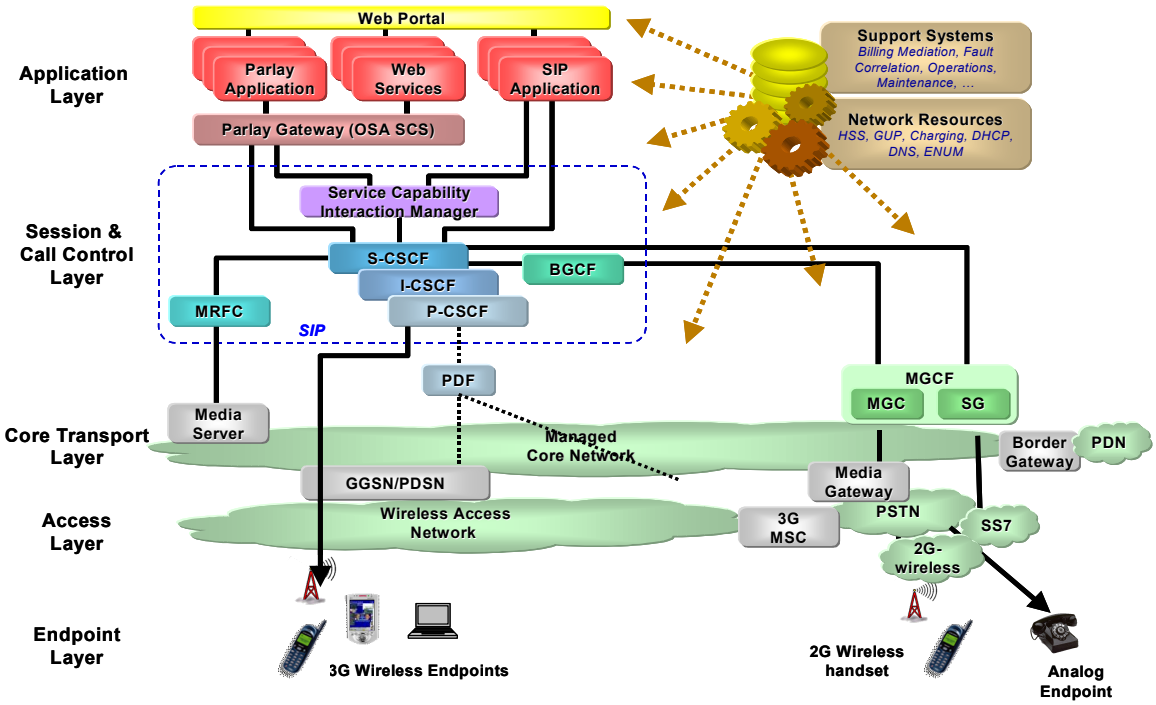


Figure 15: Wireless Architecture for Future Networks

25 Developed by the Parlay group (www.parlay.org), PARLAY is an open programming interface to a service provider's network.

For the sake of clarity, a more detailed view of the UMTS network is provided below (see Figure 16). There are NodeBs, which provide the air interface to mobile terminals and act as an entry point to the backhaul network. Radio Network Controllers (RNCs) control and manage the radio resources across NodeBs. Together they form the UMTS Terrestrial Radio Access Network (UTRAN). Beyond the RNC, Circuit Switched and Packet Switched (CS and PS) traffic are split in the ATM network. The 3G-MSC handles CS traffic and PS traffic is handled by the Serving GPRS Support Node (SGSN).

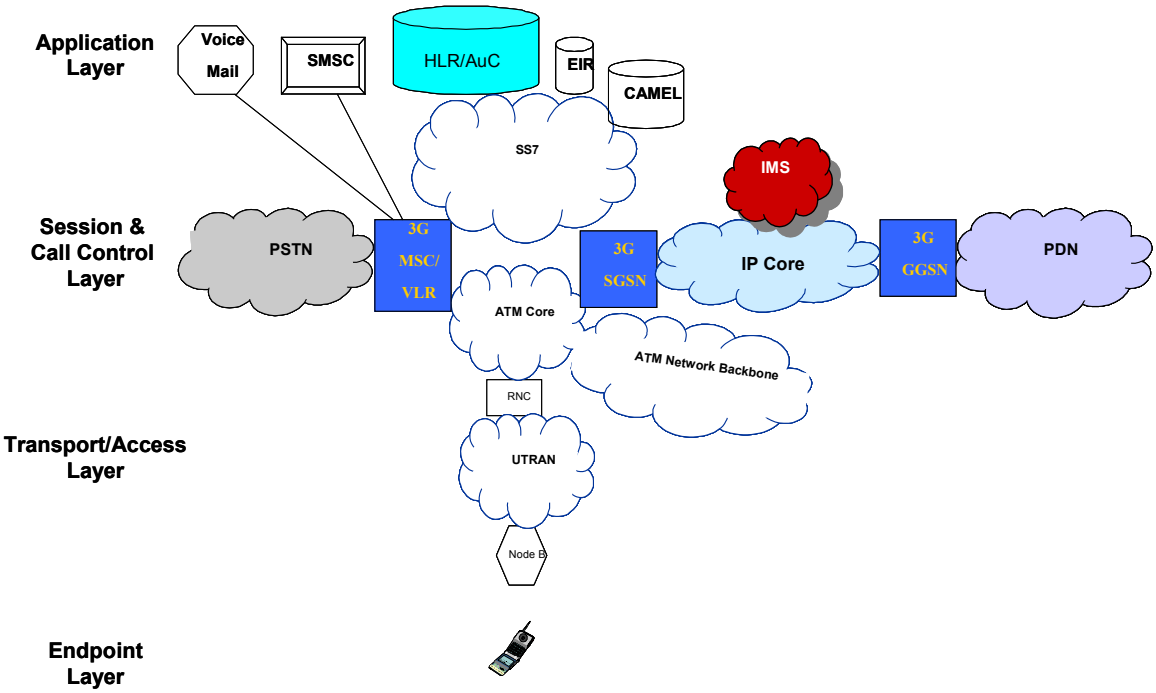


Figure 16: Rel99/Rel4 UMTS Network

In Release 99 architecture of UMTS, the 3G MSC is a single entity. In Release 4, the call control and bearer path is split into MSC server and Media Gateway (MGW) and these two entities need not be in physical proximity to each other.

The UMTS Terrestrial Radio Access Network (UTRAN) is often comprised of “star” or “tree” architecture (see Figure 17). In the star architecture, the NodeBs are connected to the RNCs via direct links (landline-based E1s or microwave links). In the tree architecture, the NodeBs are connected to intermediate hubs and then the hubs are connected to RNCs over higher speed links (e.g., E3s or STM1s) for economic reasons.

Star Topology: **Tree Topology:**

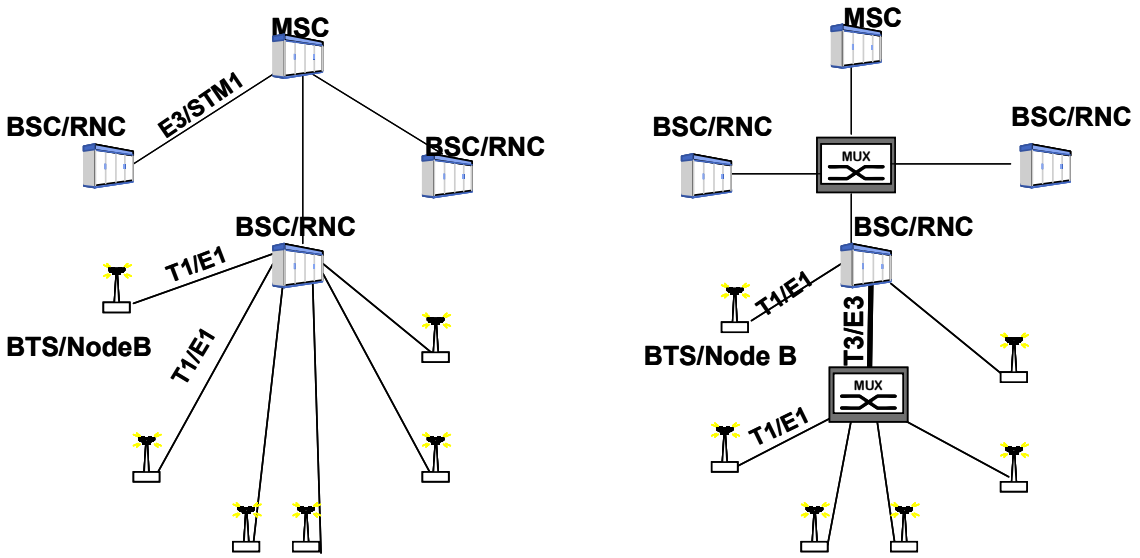


Figure 17: UTRAN Backhaul Topology

The topology chosen often depends on trade-offs between cost, reliability, terrain or other reasons. While star topology is generally expensive and results in poor facility utilisation, fault isolation is easy in this architecture. Tree structure is more cost efficient but is susceptible to high impact of a single point (i.e. hub) failure. As UTRAN evolves to IP Radio Access Network (IPRAN) in UMTS Release 6 and beyond, generic IP network architectures will represent the UTRAN backhaul network.

The RNCs are often collocated with MSCs or are connected to them via optical rings. An MSC may be supporting several RNCs. Similarly several RNCs may be connected to a SGSN and there may be many-to-many relationship between SGSNs and GGSNs which are connected to each other via an IP network (see Figure 18).

The MSCs are generally connected to each other via a mesh or a hierarchical network. The top tier of the hierarchical network is generally a full mesh configuration. The traffic from the PSTN/IN or other Public Land Mobile Network (PLMN) often enters via a Gateway MSC (GMSC), which has the capability of querying the Home Location Register (HLR) about the location of the called subscriber.

The IMS components belong to the core IP network.

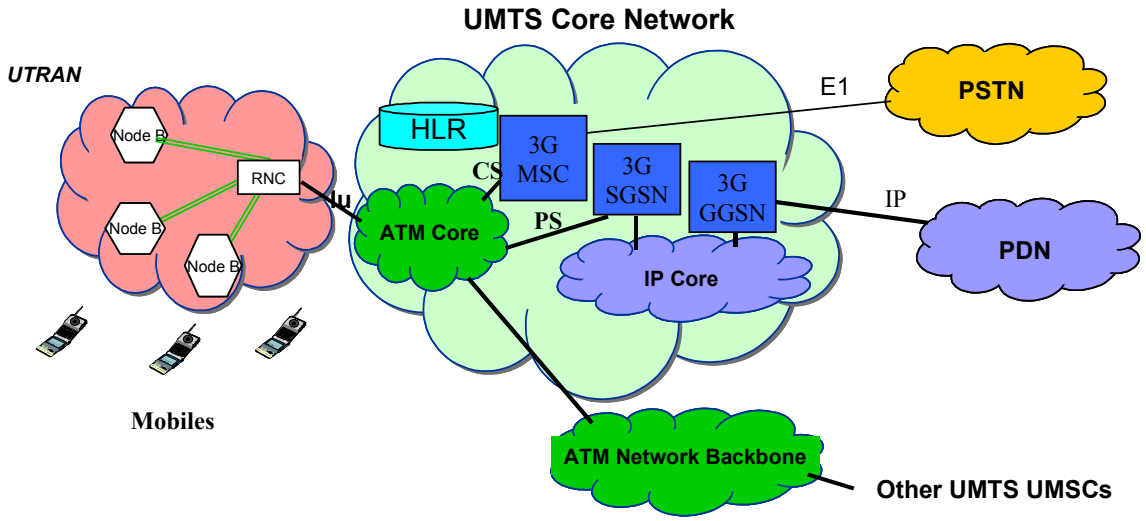


Figure 18: UTRAN & Core Network

2.2.6. Major Components of a 3G Network

For the sake of clarity, the components are broken down into two categories – core transport network and access network. A number of components in the IP Core are common across the in-scope technologies and they have been described in Section 1.1. The access network components are described below.

- **Mobile-services Switching Centre (MSC):** The MSC constitutes the interface between the radio system and the fixed networks. The MSC performs all necessary functions in order to handle the circuit switched services to and from the mobile stations. The MSC may also act as a Gateway MSC (GMSC) when it queries the HLR to obtain the location information of a subscriber so that a call can be properly routed in the network.

- **AuC:** The Authentication Centre (AuC) is an entity, which stores data for each mobile subscriber to allow the International Mobile Subscriber Identity (IMSI) to be authenticated and to allow communication over the radio path between the mobile station and the network to be ciphered. The AuC transmits the data needed for authentication and ciphering via the HLR to the VLR, MSC and SGSN which need to authenticate a mobile station.

- **EIR:** The Equipment Identity Register (EIR) is the logical entity that is responsible for storing in the network the International Mobile Equipment Identities (IMEIs), used in the GSM system. The equipment is classified, as "white listed", "grey listed", "black listed" or it may be unknown. The main purpose is to identify the use of stolen or unauthorised handsets.

- **GGSN:** The Gateway GPRS Support Node (GGSN) is the interface between the core and access networks. It acts as a point of attachment for all mobile subscribers under its coverage area. It assigns PDP addresses to all subscribers. It also acts as Policy

Enforcement Point (PEP), by interacting with the PDF and allowing packet flows based on policies implemented by the operator.

- **HLR:** The Home Location Register (HLR) is a database in charge of the management of mobile subscribers. A PLMN may contain one or several HLRs: it depends on the number of mobile subscribers, on the capacity of the equipment and on the organisation of the network.

- **SGSN:** The Serving GPRS Support Node (SGSN) essentially acts as a "MSC" for a GPRS and EDGE or UMTS Packet Switched (PS) domain. It supports packet routing to the mobile subscribers and also keeps track of all subscribers currently registered in the network under its control. It plays a key role in providing Quality of service (QoS) for packet subscribers.

- **SMSC:** The SMS Inter-working MSC (SMSC) acts as an interface between the PLMN and a Short Message Service Centre (SC) to allow short messages to be submitted from Mobile Stations to the SC. The choice of which MSCs can act as SMS Inter-working MSCs is a network operator matter (e.g., all MSCs or some designated MSCs).

- **VLR:** The Visitor Location Register VLR is in charge of an MSC area and controls a mobile station roaming in that area. The VLR maintains a local copy of the HLR data pertaining to a subscriber. The VLR and the HLR exchange information at the time of registration to allow the proper handling of calls involving a mobile station. A VLR may be in charge of one or several MSC areas.

2.2.7. Brief Description of the underlying Technology

An important aspect of 3G wireless technologies is packet-based infrastructure as opposed to a circuit-based system in the 2G technologies. Some underlying aspects of packet technology that are important for the purpose of this document are presented in this section.

2.2.7.1. Signalling and transport protocols

The core network is driven by the concept of IMS, a technology originally developed by 3GPP for UMTS Release 5 and later adopted by 3GPP2 for CDMA. IMS essentially builds on several IETF protocols to deliver IP-based high-speed data services to mobile end-points.

SIP is the primary signalling protocol in the network for both end-points as well as network elements. It allows the signalling entities to establish session parameters that are exchanged among them to establish the Quality of Service (QoS) for a session. The CSCF is at the heart of all signalling communication. Parlay or other non-SIP applications interact with entities in the IMS network through an Open Services Architecture (OSA) gateway. The primary protocol used by the HSS is DIAMETER[26].

26 An authentication, authorisation and accounting protocol for applications such as network access or IP mobility. It is a base protocol that can be extended in order to provide authentication, authorisation and accounting services to new access technologies. DIAMETER is intended to work in both local and roaming authentication, authorisation and accounting situations.

All bearer traffic is carried over IP. 3GPP does not specify the layer 2 technology, which is typically a choice between PPP, MPLS, Ethernet, POS or ATM.

The access network is based on ATM in UMTS Release 99, Release 4 and Release 5 architecture. In Release 6, the access network evolves to IP.

2.2.7.2. Subscriber Identity

In current networks, calls are routed in the networks based on the called parties Mobile Subscriber Integrated Services Digital Network (MSISDN) number. In future networks sessions will be addressed based on the subscribers SIP URI (Universal Resource Identifier). For routing traffic between the circuit and packet networks, the ENUM database will be required in addition to the traditional DNS and DHCP servers. The ENUM database will perform the translation between MSISDN and SIP URI.

2.2.7.3. Mobility & Authentication

A key component of wireless networks is the HLR or HSS, which keeps track of the subscriber whenever the subscriber is registered on the network. Whenever a mobile endpoint powers up in a network, the HLR or HSS will have to be informed about its location. This information is needed for all mobile terminated calls and sessions.

In current networks, the HLR is often coupled with an AuC. The AuC provides the authentication information so that the mobile can make or receive calls. In future networks, the equivalent function is provided by the HSS. The authentication function is built into the system in the form of an AAA server.

The HLR and HSS often serve a number of MSCs and thus store a large volume of subscriber data. If the HLR or HSS goes out of service, all subscribers will lose their service.

2.2.7.4. Quality of Service

A key driver for future network technology is high-speed data services. Since packet services do not provide dedicated connections to end-users, providing the right QoS per the user's subscription as well as per applications requirements can be a challenge. And without the right QoS, customer satisfaction cannot be achieved.

There are numerous aspects of QoS (e.g., session set up time, completion rates, and hand-off failures), which are common to both current and future networks. In this document we will consider a few aspects that are particularly relevant to future networks. 3GPP has identified four classes of service for mapping different applications. Each class has the throughput delay, jitter and packet loss probabilities associated with it (see Table 1). The network needs to provision for the right resources.

Table 1: 3GPP Class of Service Definitions

Application		Degree of symmetry	Data rate	Key performance indicators and target value		
				One-way delay	Delay variation	Information loss
Conversational	Voice	Two-way	4–128 kbit/s (4.75–12.2kbit/s AMR rate)	< 150 msec preferred < 400 msec limit	< 1 msec	0.5% FER (with graceful degradation)
	Video	Two-way	24–384 kbit/s	< 150 msec preferred < 400 msec limit	< 1 msec	< 1% FER
	Interactive game	Two-way	0–384 kbits/s	< 250 msec	< 2 msec	0
Streaming	Voice	Primarily one-way	4–128 kbit/s (32–128 kbit/s will be used within the band)	< 10 sec	< 10 msec	0.5% FER (with graceful degradation for higher FER)
	Video	One-way	24–384 kbit/s	< 10 sec	< 10 msec	< 1% FER
Interactive	Voice (messaging)	Primarily one-way	4–25 kbit/s	< 1 sec for playback < 2 sec for record	< 10 msec	< 3% FER
	Data	Primarily one-way for web browsing, email, ftp, etc	0–384 kbits/s	< 4 sec / page	N/A	0
		Two-way for database retrieval e.g. e-commerce	0–384 kbits/s (often small data volumes involved)	< 4 sec	< 500 msec	0
Background	Data	Primarily one-way	Best effort	30 sec	N/A	0

Service providers or equipment vendors often take these requirements and fit them into their own customised solutions.

While there may be different implementations of the same service by different equipment vendors, it is important that end-user experience is not compromised.

2.2.8. Characteristics Regarding 3G Wireless

The GGSN connects to the packet data network, including the Internet and is vulnerable to Denial of Service (DoS) attacks. With most networks in Europe, a few GGSNs connect to the external network. If the GGSN is out of service, the whole packet service business of the operator is affected. Since the GGSN acts as an anchor point for a very large number of subscribers (typically 100's of thousands or even millions), it can be very damaging for the operator if it became unavailable.

Appropriate security and threat management systems should be in place between the GGSN and the external data network. Service disruption can have the following impact:

- Impact on end-points: Customers will have no data service, including connections to corporate intranets, VoIP etc.
- Impact on service via other networks: Critical communication (including Instant Messaging, and video conferencing) from customer's associates will be lost

There is no standards-based protection against hacking from service provider's own customers. In traditional networks, the network elements use signalling (e.g., Mobile Application Part (MAP), Base Station Subsystem Application Part (BSSAP), ISUP based on C7) that is completely protected from subscribers. However, that is not the case with future network elements as the same SIP signalling is used towards both end-users as well as network elements. Proficient hackers can take advantage of this situation to attack and take down important network elements (e.g., CSCF), hijack calls or data too.

Appropriate security and threat management systems are to be in place between the Radio Access Network and the Core Network to prevent service disruption from occurring and having the following impact:

- Impact on end-points: Customers will have no IMS service, including connections to VoIP, Multimedia Messaging Service (MMS) etc.
- Impact on service via other networks: Critical communication (including Instant Messaging, and video conferencing) from customer's associates will be lost.

Today's HLRs and HSSs often contain subscriber data for a very large population. A site disaster can result in widespread service outages across the network. Many operators in Europe use vendor equipment for HLR that are built on high-availability platforms. Use of HLRs in a geographically redundant configuration is not very common. While reliable platforms do protect against equipment failures, they cannot withstand site disasters. There are equipment vendors who do provide geographical redundancy, but operators have not widely adopted them because of cost or other reasons.

Geographical redundancy for large HLR and HSS deployment is critical. A site disaster, either natural or man-made, can cause loss of service to millions of subscribers. This will impact service in the following ways:

- Impact on end-points: Customers will have no service at all, circuit switched or packet switched.
- Impact on service via other networks: Associates will not be able to reach customer.

There is no mechanism for active and standby arrangement with CSCF in standards. This needs to be addressed in the 3GPP standards as it is beyond the scope of service providers or equipment vendors. The challenges are more difficult than for HSS described above because:

- The HLR and HSS are basically databases that deal with relatively static data and there are well-established mechanisms of keeping active-standby databases in-synch with each other. The CSCF deals with real-time data related to an on-going session and it is very difficult to replicate it on another platform.
- In case of failure of a C7/SS7 node, there are established mechanisms in standards to route the messages to an alternate node. On the contrary, a subscriber is always associated with a particular S-CSCF (according to its HSS profile data); in case that node goes down, there is no mechanism for the subscriber to be served by another CSCF. This is an issue that needs to be addressed in the 3GPP standards as it is beyond the scope of service providers or equipment vendors. Proprietary solutions will serve only temporary purposes.

Standards need to evolve for operating CSCFs in active-standby mode. A failure or a site disaster can cause loss of service to millions of subscribers. This will impact service in the following ways:

- Impact on end-points: Customers will have no IMS service.

- Impact on service via other networks: Important communication via MMS, Push to Talk over Cellular (PtoC), etc., will be lost.

3GPP has provided detailed mechanisms for providing QoS in the UMTS layer. QoS parameters from the application layer are mapped into UMTS layer by the UMTS terminals and network equipment, which are in turn passed on to the underlying transport layer. Support of those QoS requirements at the transport layer is left to vendor implementation. For example, even though UMTS has provided for 4 classes of service, the underlying ATM or IP network may support only one or two classes of service. The mapping of the 4-to-2 classes of services may work when traffic is low and there is a lot of bandwidth over-provisioning, but is not a practical solution for the long term.

Transport equipment vendors need to ensure that the QoS mechanisms in their equipment are adequate to support QoS requirements of future networks. This involves two fundamental areas:

- The transport equipment needs to be able to identify the different classes of traffic and put them in appropriate queues.
- There has to be a well designed scheduling mechanisms to provide the packets in the queue the right priority and degree of service

Equipment and link capacity sizing should recognise the fact that the busy hour may be different for different applications (see Figure 19). It is not adequate to size network equipment based on the aggregate network busy hour traffic. In traditional circuit-based networks, there is basically only one type of traffic that peaks at a given time. However, in future networks, different types of application traffic may peak at different hours and some applications may not be at their peak utilisation when the network throughput is at its highest.

For example, VoIP traffic may peak at a particular time but Internet traffic may peak at another time while the aggregate traffic may peak at yet another time. If one sizes the VoIP equipment according to the aggregate network busy hour traffic, one could be under-engineering the equipment. Network elements should be sized for aggregate busy hour for common equipment and individual busy hour for application-specific equipment.

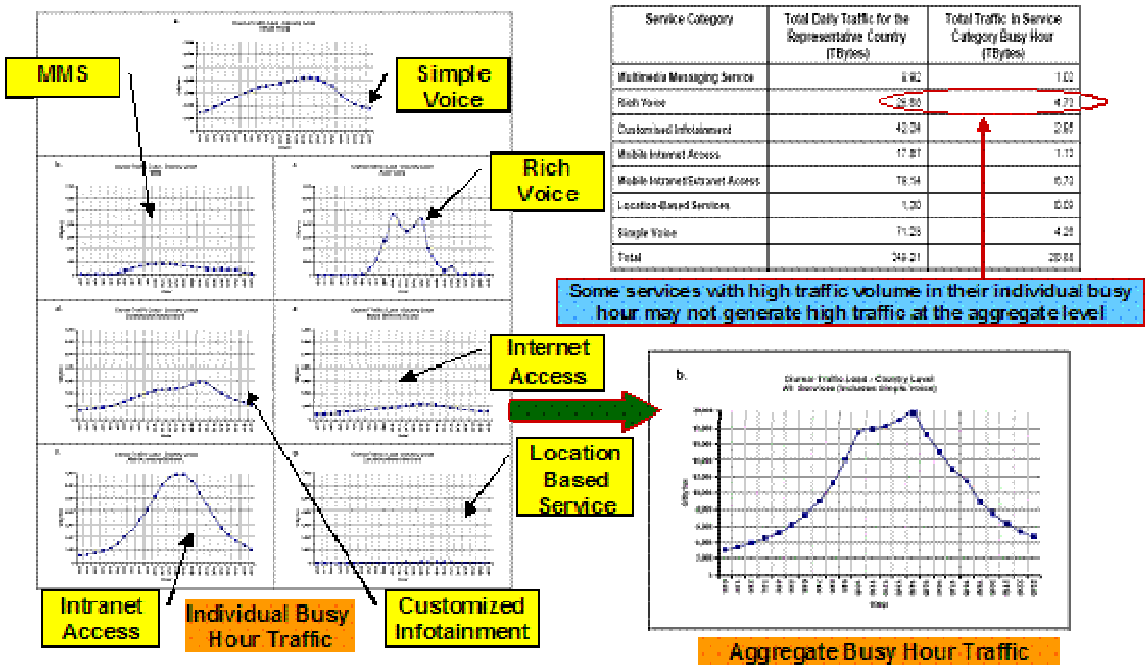


Figure 19: Aggregate Network Busy Hour & Individual Application Busy Hour

2.3. WiFi

2.3.1. Introduction

Wireless Fidelity (WiFi), a well known 802.11 standards-based technology for wireless communication, is very popular in Europe. The major areas of use are commercial hotspots, managed by Carriers and Enterprise Networks and there is also a promising UMA (Unlicensed Mobile Access) scenario, in which Operators try to offer seamless roaming feature between WiFi and cellular networks at an attractive cost. One of the pioneers in offering UMA services in Europe is BT.

Generally the WiFi today, is a widespread technology with constantly growing number of users. It had some security problems in the initial stage of standard evolution that were solved by an extension to the standard (802.11i) and appropriate awareness campaign for end users. The new version of standard, known also as WiFi Protected Access 2 (WPA2), forced vendors to introduce changes in both hardware and software offering enterprise grade security mechanisms.

2.3.2. Usage and market trends

WiFi has gained acceptance in many businesses (over a third of German enterprises have deployed WiFi across all their business locations[27]), agencies, schools, and homes (84% of UK internet users have WiFi access[28]) as an alternative to a wired LAN. Many airports,

27 Source: Lucent Primary Market Research, Evros Study Readout

28 Source: http://www.theregister.co.uk/2006/08/29/aol_wireless_survey/

hotels, and fast-food facilities, exhibition and conference centres offer public access to WiFi networks. These locations are known as hotspots. The total number of hotspots[29] in the Western European market is expected to increase at a compounded annual growth rate (CAGR) of 11.6% to 64,384 hotspots by 2010[30].

While most hotspots nowadays cover single locations (e.g., airports, coffee place), deployments of WiFi networks that provide citywide coverage (municipal WiFi networks) are gaining momentum. Worldwide deployment of municipal wireless networks for public Internet access will continue at a rapid pace over the next few years, with the US leading the way. The total worldwide market will reach 248 deployments by the end of 2006, and will grow to over 1,500 by the end of 2010[31]. In Europe, several plans to deploy citywide networks have been announced by major service providers[32].

Even though the competitive landscape to provide WiFi service is crowded, there are still new entrants making headway in this space. Some service providers came to the market with innovative business plans to provide free hotspots. In general there is no clear business plan to make money. As technology evolves (multi-hop architecture, higher bandwidth, etc.), the path to a profitable business case is more feasible. For example, one service provider uses a business model where broadband users sign up to the service and make their WiFi connection available to other members as well as paying non-members. A paying non-member (also called alien) is a member that uses the service provider's network without providing or sharing his or her own access point. The viability of the business case relies on the money that those non-members are contributing. This service provider claims to be the largest WiFi community in the world with 81,202 members (38,366 in Europe) as of August 29, 2006[33].

Recently, some operators have positioned WiFi and cellular Fixed-Mobile Convergence (FMC) solutions in the market. WiFi is considered as a fixed wireless technology. It is an alternate way to provide wireless broadband to consumers. The other way of providing the same capability is through cellular networks in conjunction with wireline networks. It is possible to bridge those two architectures by providing seamless roaming between WiFi and the cellular technologies (3G1X, UMTS, etc.). Emerging dual-mode 2G and 3G-WiFi phones allow users to switch seamlessly from a cellular to a WiFi network. Dual-mode 2G-WiFi phones are already available while 3G-WiFi phones are just being introduced in the marketplace. For example, overall 82 cellular-WiFi device types were on the European market as of end 1H06[34]. Dual-mode solutions will benefit the enterprise segment. It will provide better Return on Investments (ROI), shift telephony control back to the enterprise and provide the most integrated solution type for service and support[35].

While WiFi hotspots will continue to grow over the next few years, other technologies such as WiMAX (see Section 3.4) and 3.5G technologies are likely to influence the future

29 Only commercially deployed hotspots (free wireless networks, city networks, or community networks and enterprise networks are not included in the projection)

30 Source: IDC, Western European Hotspot LAN Equipment Forecast, 2005-2010

31 Source: http://government.zdnet.com/index.php?page_id=1816&id=1360802

32 Source: http://news.zdnet.com/2100-1035_22-6090503.html

33 Source: www.fon.com

34 Source: Informa telecoms and media, Volume 8, Issue 12

35 Source: Yankee Group, Wi-Fi and Cellular FMC Solutions Lack Market Acceptance

deployment of WiFi hotspots. As the breadth of WiFi coverage is not likely to be comparable to cellular networks, even in major markets, WiFi networks do not present an immediate threat to 3G. Vendors and service providers will have the choice to either integrate WiFi with other mobile technologies such as GSM (2G), UMTS (3G), High Speed Downlink Packet Access (HSDPA) (3.5G) and WiMAX or develop different network topologies (i.e. mesh networks), which would provide better financials for WiFi networks. The viability of wide area WiFi deployments has been largely constrained by backhaul requirements to connect large number of WiFi access points. Mesh technology has provided a mean to solve this issue. Utilizing a series of WiFi nodes within close distances of each other, WiFi mesh technologies reduces backhaul costs by permitting several WiFi nodes to share one backhaul connection.
With the growing penetration of WiFi access point in households, the burgeoning of municipal and free WiFi networks, the proliferation of roaming agreement between cellular and WiFi providers, and the strong acceptance of WiFi solutions in corporations, the future deployments of WiFi solutions is bright. However, security, quality of service and robustness of those networks, if not addressed, will affect negatively the future growth and acceptance of this technology.

2.3.3. Wireless Networks Architecture

A WiFi network is a Wireless Local Area Network (WLAN) that uses airwaves as information medium allowing for a flexible, cost-effective way of expanding network resources. Additionally thanks to mobility of the solution it makes the WLAN scalable and easily extensible.

The typical architecture for a WiFi wireless network is presented below (see Figure 20). The basic components of wireless architectures are wireless station (STA) and wireless Access Point (AP). The Access Point maintains relation with connected STAs, which is called association. The connection initiation (association) takes place when the following conditions are met:

- Wireless station is in range of an access point and the signal strength and signal to noise ratio is sufficient to exchange traffic.
- Station and access point are using the same radio channel and transmission speed.
- Station is able to authenticate with AP.

Wireless communication can be established in the following modes of operation:

- Infrastructure Access, where users have wireless network cards and connect to APs to obtain network access. The AP is acting like network bridge between wired network and wireless domain. Access Point is responsible for managing the communication and Stations associations.
- Ad hoc Access, where wireless stations establish connections with each other without the mediation of an AP.
- Network Backhaul, where wireless equipment is used in order to extend networks. In this scenario, wireless devices work like transparent bridges and are used to interconnect different networks. Also, there is no individual user authentication as it is the transport segment of the network.

The topology of a WLAN is described below:

– Hub-spoke topology, where an AP plays the role of a Hub and Wireless Stations act as spokes. The AP is a central entity that associates and manages wireless stations.

– Point-to-point topology, typically used in wireless bridging applications. In case of wireless bridging, either point-to-point or point-to-multipoint topologies can be considered depending on the application requirements.

WiFi devices operate in license free band and have limitation for output power of radio emission. Thus, the typical coverage range is rather small and is limited to 20-40m inside buildings and up to 100m in open space areas. In case of point-to-point connections with special dish antennas, offering appropriate signal gain, ranges can span to 2-3 km but they are still restricted by available power emission level (limited by regulations), line of sight and interferences.

Generally, the most popular application scenario is hub-and-spoke, infrastructure mode.
In this scenario we can use the wireless AP as:

– A LAN extending device, where AP is acting like a hub connected to the network core. This type of scenario is used by enterprise, public hot-spots, internet café and service providers for Unlicensed Mobile Access (UMA).
– A wireless residential gateway, AP is also acting as a WAN router providing Internet or corporate network access and often network address translation for wireless users. This type of scenario is mostly found in residential home applications.

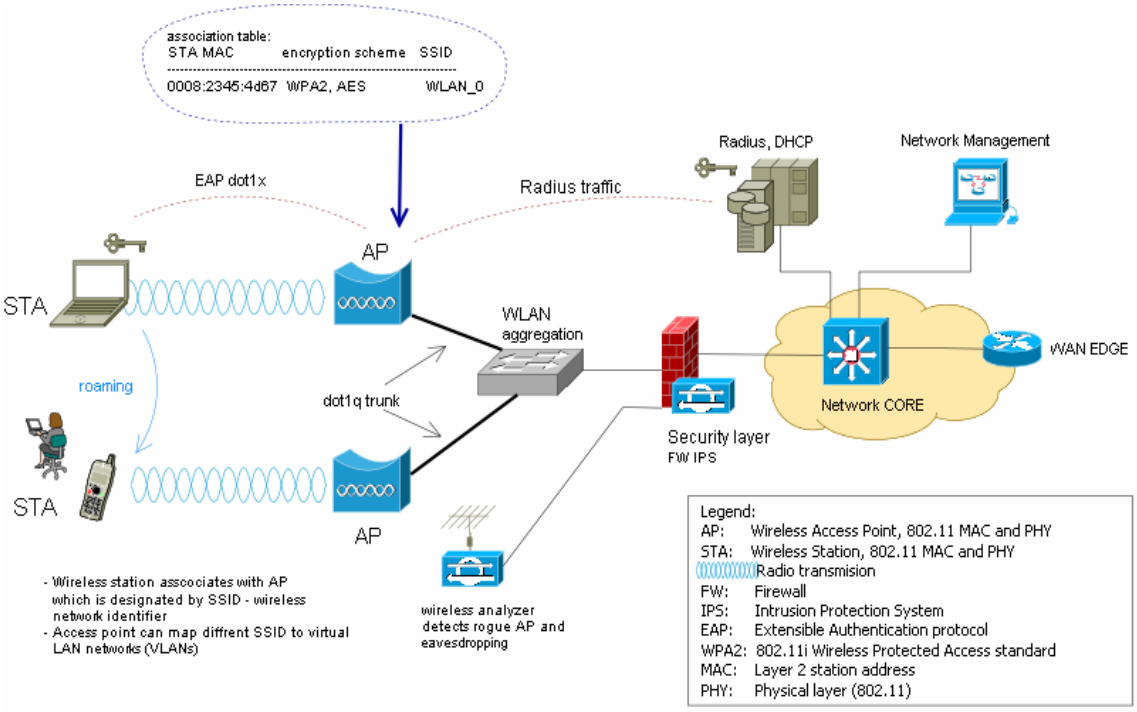


Figure 20: WiFi Architecture Overview

Wireless technologies are easily accessible medium and thus they are prone to eavesdropping. To alleviate this drawback it has to be compensated with the following security controls that are represented by appropriate architecture elements:

- Confidentiality and Integrity protection. STA and AP using appropriate hardware and firmware.
- Wireless monitoring. Wireless analyzers and management software allow for rogue AP and STA detection and interference analysis.
- Authentication, Authorisation and Accounting. Access Point (Authenticator) and additional Remote Authentication Dial In User Service (RADIUS) server (Authentication Server).

2.3.4. Major Components of a WLAN

The WiFi Wireless Local Network (WLAN) consists of two classes of devices: radio equipped devices and support systems.

Radio equipped devices include STAs and distribution system devices (i.e. APs) that offer services for stations. Support systems assist wireless distribution devices in authentication and are also responsible for the device management. Support systems also include security control functions like wireless probes and intrusion detection systems.

Following is the list of typical elements of the WLAN:

AP: The Access Point (AP) is a wireless device that provides network access services for wireless stations.

Authentication Server: The Authentication Server is a RADIUS server that performs the 802.1X Extensible Authentication Protocol (EAP) authentication process and automatic key management for the STAs.

Management Station: The Management Station is a system that allows for detection of wireless problems from the data sent by wireless probes.

Wireless Analyzer: The Wireless Analyzer is a wireless probe that collects events from wireless operations. It gathers information from every channel of available WiFi band and sends updates to the Management Station.

Wireless Repeater: The Wireless Repeater is a wireless device that enables wider coverage of the AP by regenerating frames. Usually it is equipped with an additional antenna. It works only on the physical layer level.

Wireless Residential Gateway: The Wireless Residential Gateway is an access point that also serves as a WAN gateway. It is used typically in residential applications.

Workgroup Bridge: The Workgroup Bridge is a wireless access point that associates as a client to another access point. All client stations are represented by the physical address of Workgroup Bridge in the network.

STA: The Wireless Station (STA) is end user equipment, which associates to an Access Point. Examples of device types include:

- PC computers and laptops with WiFi card (PCMCIA, PCI, CARDBUS)
- PDA devices
- Smart Phones and GSM devices with wireless cards

2.3.5. Brief description of Underlying Technology

WiFi (802.11) family of standards includes the following:

802.11, operating at 2.4GHz band, 1 or 2 Mbps bandwidth achieved with Frequency Hopping Spread Spectrum (FHSS) or Direct Sequence Spread Spectrum (DSSS) modulation over infra red link. 802.11 has never been implemented.

802.11a, operating in 5GHz band, offering 54Mbps maximum bandwidth, using 52 sub channels in Orthogonal Frequency Division Multiplexing (OFDM) technology with 12 non-overlapping channels, used in North America and Japan

802.11b, operating in 2.4GHz band, maximum 11Mbps bandwidth using complementary code keying (CCK) modulation over 14 5MHz channels (depending on country) and 3 non overlapping channels, used in Europe and Japan. It uses CCK for 11 and 5.5 Mbps speed and DSSS for 1 or 2Mbps mode.

802.11g, operating in 2.4GHz, maximum speed of 54 Mbps due to OFDM modulation, compatible with 802.11b, used in Europe and Japan. In detail 802.11g can adapt to conditions by adjusting speed and modulation: It uses OFDM for 6, 9, 12, 18, 24, 36, 48, and 54 Mbps, than CCK for 11 and 5.5 Mbps and finally falls back to 2 or 1 Mbps with DSSS.

802.11i, WPA2 amendment, known also as Robust Security Network (RSN). This standard enforces the use of Advanced Encryption Standards (AES), utilizing the Rijndael cipher in counter mode for confidentiality, and AES in Cipher Block Chaining mode (CBC) for sake of integrity protection.

802.11n, in active development, working in 2,4 or 5GHz band and with speeds up to 540Mbps.

802.11r, will permit connectivity aboard vehicles in motion, with fast handoffs from one base station to another managed in a seamless manner to support real time services such as voice and video.

802.11b and 802.11g divide the 2.4 GHz spectrums into 14 overlapping, channels whose centre frequencies are 5MHz apart. The 802.11b and 802.11g standards do not specify the width of a channel; rather, they specify the centre frequency of the channel and a spectral mask for that channel.

WLAN networks use Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) as the medium access method, which provides contention-based access.

Wireless devices form Basic Service Sets that involve one or more members that share common coordination function. There are two types of Basic Service Sets:

- Independent Basic Service Sets (IBSS) known also as ad hoc type network which does not require AP (Distribution System)

- Enhanced Services Set (ESS), which is an extended Basic Service Set, that involves more then one BSS interconnected by a distribution system (either wired or wireless). IBSS or ESS is also known as infrastructure or enterprise network

Wireless stations can discover available wireless networks by sending probe packets (active scanning) or listen to beacon frames (passive scanning) transmitted by APs usually every 100ms. Beacon frames contain the information on configured Service Set Identifiers (SSIDs) that identify the network, supported rates and available security mode. STA chooses the AP with the best available radio parameters (signal strength). In the next step the STA tries to associate to an access point. Before that happens the STA needs to authenticate with the AP. There are two methods of association authentication:

- Open systems authentication, no additional connection set-up is needed. The station is expected to send encrypted packets with appropriate key. This method is considered to be the more secure of the two available.
- Shared access authentication, challenge and response method that requires associating party to respond with an encrypted challenge send to the AP. This method is not considered secure as it gives away information that enables key derivation. In particular the observer sees plain text message and its encrypted version. This method has been discarded from 802.11 standard as pointless.

2.3.6. WiFi Security

Packets sent via wireless medium, due to the nature of airwaves, can be easily captured and inspected. To address this issue the original 802.11 standard had specified Wired Equivalent Privacy (WEP). WEP uses RC4 cipher to provide confidentiality and CRC-32 to provide integrity. WEP is able to use two key lengths: 64 and 128 bit. The real key length is limited to 40 and 104 bit as 24bit is used for the Initialisation Vector used to provide key stream for RC4 stream cipher.

WEP has been proven to not provide adequate protection and is now treated as an obsolete protocol. The weaknesses of WEP include:

- Small IV space and IV collisions
- Weak IVs
- Susceptible to packet replay injection
- Weak integrity protection, packets can be modified without having the WEP key
- Lack of key management, the key is static, shared by STA and AP

As an intermediate response to those problems the WiFi protected Access (WPA) has been proposed, known also as Transient Secure Network (TSN). It mandates the use of RC4 with 128bit key and 48bit IV. It uses Temporary Key Integrity Protocol (TKIP) for changing keys while data is transmitted and Michael the Message Integrity Code (MIC) scheme to counter replay attacks and provide integrity.

The WPA is designed to work with 802.1x network authentication method offering automatic key management and advanced authentication although it is also possible to use it in WPA Personal mode that uses pre-shared keys. In 802.1x mode besides the STA and the AP an Authentication Server is required. It usually is a RADIUS machine that is able to establish EAP sessions with wireless stations. The EAP has a variety of options offering secure authentication and key management like for example:

- Protected EAP (PEAP), uses SSL for confidentiality and MSCHAPv2 or Generic Token Cards for authentication purpose
- EAP-TLS, uses Transport Layer Security (TLS) and Public Key Infrastructure (PKI) digital certificates for authentication
- EAP-MD5, uses digital hashes, weak security

The WPA did overcome most of the weaknesses of WEP, being easily introduced on the same chips of wireless devices. Its main purpose was to make transition phase possible before launch of WPA2.

The final, most recent addition to 802.11 is the 802.11i, WPA2 amendment, known also as RSN (Robust Security Network). This standard enforces the use of AES (Advanced Encryption Standards), utilizing Rijndael (AES) cipher in counter mode for confidentiality, and AES in Cipher Block Chaining mode (CBC) for sake of integrity protection. AES – Counter Mode CBC Mac Protocol (AES-CCMP) is considered as the replacement for TKIP and Michael of WPA. The WPA2's main purpose is providing Enterprise grade security. Similarly to WPA is can be used in two operational modes:

- WPA2-Personal, personal mode with pre-shared keys
- WPA2-Enterprise, using 802.1x network authentication scheme

2.3.7. WiFi planning and operation

WLANs used to provide large space coverage have to be split into zones. Depending on the wireless standard, there are a limited number of non-overlapping channels available (3 channels for 802.11b and 802.11g – channels 1, 6 and 11). Adjacent zone pairs cannot work on the same channel.

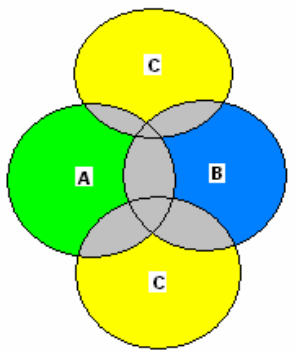


Figure 21: Wireless Channel Allocation Pattern

The concept of frequency reuse and zoning can be represented pictorially (see Figure 21). The grey areas in the figure indicate location where the wireless station will try to check which AP offers better conditions and if it is time to roam from one AP to another.

There are several techniques that enable faster roaming. The time roaming takes is important especially for low-latency services like voice and multimedia traffic. When a complex authentication scheme is used the roaming time can be significant. To address this issue APs are organised into groups that have one leader that serves as the authentication agent and session cache. Every other APs keep TCP session with agent and proxy all authentications to the leader. When wireless station changes AP the new AP queries the cache on authentication agent and associates client if the entry is found.

2.3.8. Characteristics Regarding WLANs

Wireless networks are sharing an open access medium. An important issue is inherent lack of confidentiality over the RF air interface. Use of enterprise grade security standards, like

WPA2 with high key lengths (192 or 256 bit keys), should be considered to protect the wireless traffic.

WiFi systems do not offer good quality of service solution, as they are a shared media access system where users compete for the medium. Furthermore, the wireless signal is susceptible to deliberate or weather related jamming and interference. This can be of serious impact on badly designed wireless system when there is not enough link budget allocated for risk mitigation. Due to the susceptibility of wireless signal to jamming and quality of service problem, passing critical application on wireless technology has to be carefully evaluated by Network planners. For critical application like voice, separate wireless zones (SSID) for operation should be used.

WiFi networks use two authentication methods: open-system authentication and shared-key authentication. In both methods, each mobile client must authenticate to the access point. With open-system authentication, actually no authentication takes place. The shared-key authentication, which depends on WEP, is easily breakable. Other authentication methods, such as Remote Authentication Dial-In User Service (RADIUS)[36], should be used to secure WiFi networks. Trained IT personnel can deploy these more robust authentication methods in enterprises or Wireless operators' networks.

Factory default "Out-of-the-Box" settings create an open and vulnerable network. Many wireless adapter cards on workstations come by default with wireless ad hoc mode enabled. Attackers can associate with such STAs in peer-to-peer mode gaining easy access to a vulnerable device. WiFi APs typically default to an open (encryption-free) mode. Users should change default settings prior to activating the network. Public education and awareness campaigns are needed.

Improperly placed APs in the network could lead to eavesdropping and put the entire network at risk as well as networks they interconnect with. For example if the AP positioned outside the firewall is compromised, an intruder could have their way inside the defensive ring of the firewall. Proper network planning will avoid vulnerable APs. The use of Virtual Private Network (VPN) will alleviate this problem by securing the connection between the end-user and the network.

WiFi broadcasts in the unlicensed 2.4-GHz band. There are no rules controlling the use of this frequency. This leads to WiFi pollution and frequent jamming by 'naturally' occurring radio waves, which leaves users with a less than adequate connection. Vulnerabilities found in the WiFi standard (e.g., WEP) can combine with its operation in unlicensed bands to allow malicious attackers to jam the wireless networks leading to Denial of Service. Careful network planning can mitigate the problem. When setting up their wireless APs users should avoid high-density areas such as large apartment complexes or office buildings with many Wi-Fi APs. Furthermore, network owners should change default factory settings of the AP. Many WiFi APs default to the same channel, contributing to congestion on certain channels.

Increasing use of dual cellular-WiFi phones that enable roaming from cellular networks to WiFi networks, can lead to problems due to the new technology and due to interference. WiFi-WiFi handoff from one AP to another or WiFi-cellular handoff from WiFi LAN to mobility WAN are cumbersome. Earlier versions of mobility implementations do not have efficient signalling in place. This could lead to increased delay and service disruption. In general LAN technologies are not optimised for WAN performance and roaming applications. The

36 This protocol was developed by Livingston Enterprises and is the de facto standard for authentication servers.

introduction of 802.11r will facilitate IP telephony (the term "IP telephony" refers to voice calls in which some portion of the call path is IP) by enabling faster handoffs. The latency issue will be somewhat alleviated by the new standards developed around Quality of Service (QoS). For example, 802.11e will provide media traffic prioritisation.

WiFi mesh technologies reduce backhaul costs by permitting several WiFi nodes to share one backhaul connection but it comes at the cost of bandwidth and QoS. An average of 30-40 ms is lost per hop in the meshed network making VoIP impossible after 4 hops as less than 150ms latency is needed for a good conversation. Additionally, the number of hops required before hitting a backhaul point limits mesh WiFi bandwidth. The chart below gives more details on the impact of multi hops on total throughput available to users (see Figure 22). A new standard, 802.11n, which provides more bandwidth, coverage and in-building penetration, will alleviate the intrinsic limitations of mesh networking. The latency issue will be somewhat alleviated by the new standards developed around Quality of Service (QoS). For example, 802.11e will provide media traffic prioritisation.

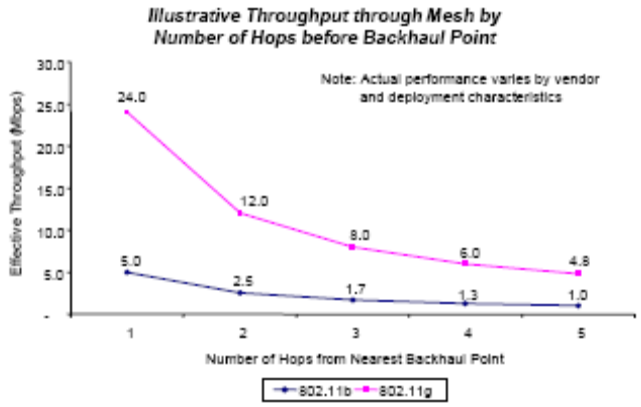


Figure 22: Throughput through Mesh by Number of Hops before Backhaul Point[37]

The security of wireless communication is affected by unwanted coverage. The quality and Wireless communication is affected by the lack of visibility between devices and can be disturbed by reflections. The line of sight is required for point-to-point long haul bridged links. Careful planning, wireless site survey for optimal placement of APs, avoiding unwanted coverage of wireless network outside the premises, adjusting power levels and analyze potential reflection problems are a[[roaches to follow.

Rogue AP attack is a common technique of breaking into a wireless network. WiFi wireless stations can easily associate with hostile devices if the security settings on that device are weak. This can lead to disclosure of information as a user believing that he is connected to proper AP commences communication. Providing wireless network management through wireless IDS or IPS can enable rogue STA and AP detection through wireless performance and coverage reporting.

An attacker can use a badly configured wireless card as gateway to the network. Steps to reduce the chances of such attacks include the use of advanced network access authentication mechanisms (like 802.1x with secure EAP methods) and placement of firewall

37 Source: Bearn Stearns, Meshed WiFi Impact Assessment: Notes from Call with Industry Consultants - CSMG

on the border of the wired network. Allowing traffic on a need to know basis only and adoption of zoning will minimise break-in consequences.

2.4. WiMAX

2.4.1. Introduction

Worldwide Interoperability for Microwave Access (WiMAX) is an emerging Institute of Electrical and Electronics Engineers (IEEE) 802.16 standards-based technology that is still in its early stage of evolution. WiMAX offers the following remarkable advantages for service providers and carriers:

- Provides an alternative to DSL and Cable in high-speed data access
- Pushes the high-speed data footprint beyond DSL's reach especially in terms of distance
- Provides lower backhaul cost for cellular and WiFi networks
- Meets the bandwidth and QoS requirements of both residential and business users

WiMAX is an interesting alternative for East European operators as they do not have full coverage for their cellular networks and this technology is a cost effective way to extend it. Operators in the West European countries, who generally do have the adequate coverage, can use WiMAX to provide more bandwidth for new bandwidth demanding services (e.g., multimedia services, Internet access). For the West European operators, WiMAX is an opportunity to build backhaul networks that are more cost effective to manage than a wired counterpart.

2.4.2. WiMAX Usage and Market Trends

Projections are that WiMAX installation in larger numbers will begin in 2007 with the five year (2005 to 2009) compound annual growth rate (CAGR) for base stations to be about 94% in Europe, the Middle East and Africa (EMEA). The total deployed numbers are still significantly less than the cellular base stations already installed. It is estimated that by 2009, 23,600 WiMAX base stations will be installed in the EMEA region with 633,000 Customer Premise Equipment (CPE) devices talking to those installed base stations[38].

The development of the standards, release of spectrum, and operational issues will determine the WiMAX roll out pattern. WiMAX is an emerging technology being supported by multiple industries. For example, the Personal Computer industry is looking to install WiMAX access devices in the base offering, which will promote the roll out of WiMAX networks to enable the population to use the functions.

From the WiMAX equipment vendor perspective the combined Europe, Middle East and America revenue projections for the five years from 2005 to 2009 are estimated in the US$2.1B range broken out by US $1.6B for CPE and US$ 0.4B for base stations.

38 WiMAX and Outdoor Mesh Equipment, Quarterly Worldwide Market Share Forcasts for 2Q06," Richard Webb, Infonetics Research, June 2006.

2.4.3. WiMAX Architecture

WiMAX, 802.16, is a relatively new standard as it has been first approved in December 2001. The WiMAX forum first certified equipment in January of 2006 (Wave 1 – radio interface compatibility). The idea of WiMAX is to deliver Broadband Wireless Access (BWA) in a cost-effective way. Whereas WiFi is a LAN technology, WiMAX generally is a Metro Access Network (MAN) technology with expected range counted in kilometres. The main applications of WiMAX are:

- End-user access for Internet and local loop, still not ready for deployment
- Backhaul (cellular networks and hot spots). It can extend WiFi networks by providing low cost backhaul connections
- Public safety and monitoring
- Enterprise networking (campus)

The typical application scenarios are depicted below (see Figure 23).

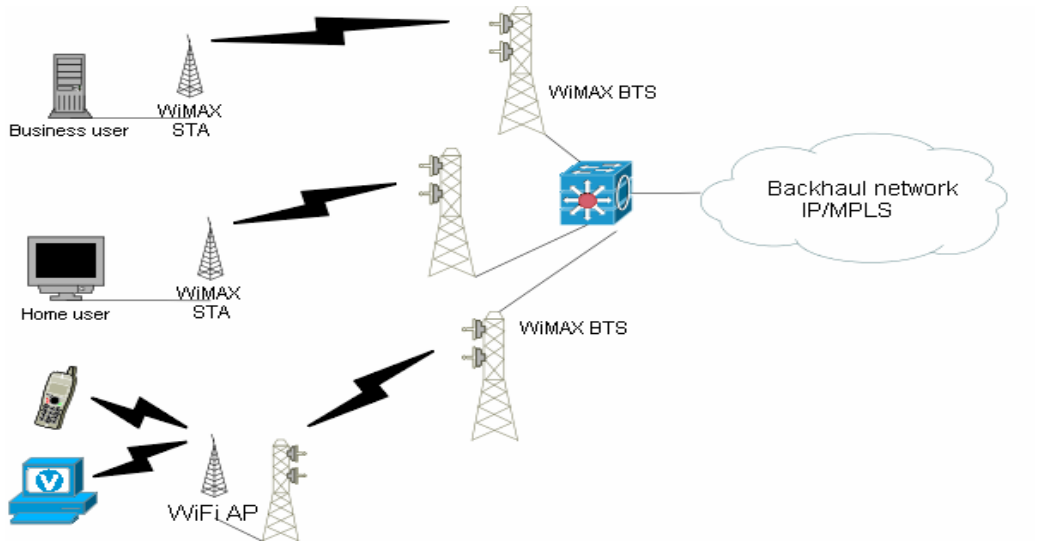


Figure 23: WiMAX Architecture Overview

The 802.16 standard has gone through several amendments, the most important being:

- Fixed MAN (described in amendment 802.16d). Provides higher bandwidth, range (75Mbit, 4-6 miles), and can work in point-to-multipoint and mesh structures.
- Portable MAN (described in amendment 802.16e). Provides a range of up to 3 miles and bandwidth up to 15Mbits. It is the most recent addition to the 802.16 family. It adds the mobility component to the standard and allows for fixed wireless and mobile Non-Line-Of-Sight (NLOS) applications.

802.16 is a point-to-multipoint technology. WiMAX Base Station serves as the access point and manages stations connected to it. 802.16 technology uses three types of modulation: QPSK, QAM16 and QAM64 in order to cover appropriate ranges and allow flexible wireless planning (larger area can be covered at a slower acceptable speed).

WiMAX can be deployed in two modes:

- **Fixed WiMAX** scenario. This scenario is typically used in low-density suburban and rural areas with large-sized cells and large area coverage. Typical applications include inter-connecting WiFi hotspots with each other, and with the Internet. Fixed WiMAX also provides a wireless alternative to cable and DSL for the last mile broadband access.
- **Portable WiMAX** scenario. This scenario is typically used in high-density suburban and urban areas with small-sized cells with selective coverage (hot zones). It is employed for fixed and portable services using indoor (self-install) CPEs and portable devices (Laptops).

In dense urban areas fixed WiMAX can work in mesh mode creating resilient and robust networks resistant to node outages (see Figure 24).

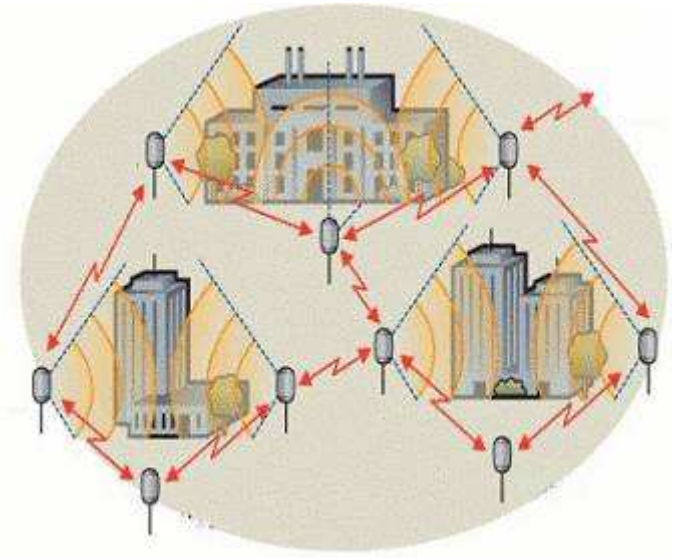


Figure 24: WiMAX Mesh Topology

WiFi and WiMAX can be combined to create a complementary solution for large area coverage without the use of expensive wired solutions. One example is WiFi providing wireless access for the last mile and WiMAX being used to provide a non-wired backhaul to a centralised location.

2.4.4. Major Components of WiMAX Networks

- **WiMAX Base Station:** The WiMAX Base Station is a hub station associating Customer Premises Equipment (CPE) devices and end-users stations.

- **WiMAX CPE:** There are two types of WiMAX Customer Premise Equipment (CPE):
  - In-door fixed station
  - Mobile station.

- **WiMAX Management:** The WiMAX Management is a dedicated application for network element management.

2.4.5. Brief description of Underlying Technology

The WiMAX spectrum available in Europe ranges from 2.3 GHz to 5.8 GHz. Other frequencies that are used in Europe are:

- 3.7 GHz band
- 2.6 GHz band

The 5.8 GHz band is unlicensed in most of the world.

The original WiMAX standard (IEEE 802.16) specified WiMAX in the 10 to 66 GHz range. The 802.16-2004 amendment, also known as 802.16d, added support for the 2 to 11 GHz range and was updated to 802.16e in 2005. The 802.16e revision uses scalable orthogonal frequency-division multiplexing (OFDM) as opposed to the non-scalable version used in revision 802.16d. This brings potential benefits in terms of coverage, power consumption, frequency re-use and bandwidth efficiency. Revision 802.16e also adds a capability for full mobility support.

The WiMAX specification improves upon many of the limitations of the WiFi standard by providing increased bandwidth and range as well as stronger encryption. It provides connectivity between network endpoints without the need for a direct line of sight in favourable circumstances. The NLOS performance requires the 802.16d or 802.16e revisions, since the lower frequencies are needed.

WiMAX certification is a process that's comprised of gradual steps, called "Waves". The certification process was started in November 2005 and is due to be executed over 2006 and 2007. A completed certification process will aid the implementation of reliable and secure solutions. In January 2006 the first products were certified as of Wave 1.

- Wave 1: radio interface interoperability certification
- Wave 2: certification of service profiles, quality of service, network security for fixed topologies (non mobile)
- Wave 3: fixed and portable network certification, end-to-end QoS, 802.16e certification
- Wave 4: mobile and portable products certification

Contrary to the WiFi systems that use contention access (i.e. every STA associated to an AP is sharing its available bandwidth), WiMAX systems use scheduler mechanisms. There are two mode of operation: Frequency Division Duplex (FDD) using channels; and Time Division Duplex (TDD) using time slots. This makes 802.16 technologies better suited for backhaul scenarios, as quality of service is inherent in technology design.

Table 2: TDD vs FDD

	TDD	FDD
Advantages	→ enhanced flexibility as channel allocation is easier → asymmetrical	→ proven for voice → designed for symmetrical traffic
Disadvantages	→ cannot transmit and receive at the same time → it is essential to synchronise base station with CPE device	→ cannot be deployed when spectrum is unpaired → spectrum is licensed → higher costs of spectrum licensing

TDD is intended for asymmetrical data applications, environments with unstable traffic patterns and when frequency allocation is rigid. TDD enables 100% use of available

spectrum. It enables advanced technologies such as mesh network and adaptive antenna arrays, more suitable for modern IP protocols equivalent. FDD is used in predictable traffic patterns and when equipment cost is important (see Table 2).

According to the specification, WiMAX portable standard 802.16e characteristics are:

- High Data Rates – divided into sub-channels, Advanced Coding and Modulation
- Quality of Service (QoS) – optimal scheduling of space, frequency and time resources over the air interface on a frame-by-frame basis
- Scalability – channel width from 1.25 to 20 MHz, TDD
- Security – EAP-based authentication, AES-CCMP-based encryption, and CMAC and HMAC based control message protection schemes; support for SIM and USIM cards, Smart Cards, Digital Certificates, and Username and Password authentication methods
- Mobility – optimised handover, latencies < 50ms, real-time applications (VoIP), key management; vehicular speeds greater than 120 km/h

2.4.6. Characteristics Regarding WiMAX

Wireless Network are sharing an open access medium, thus their most important issue is inherent lack of confidentiality without the use of any data encryption technique. Confidentiality of information traversing wireless networks depends on the strength of encryption methods used. Software implementation quality and resistance to attacks is vital.

As wireless media is insecure and the risk of loss of confidentiality is high, network owners should perform appropriate risk analysis before deploying wireless network technologies. Implementation of the following recommendations will help improve wireless security:

- WiMAX is still undergoing evolution so it is advised that proper acceptance tests are performed before deployment.
- WiMAX fixed 802.16d requires proper link budget calculations and wireless planning.
- The vendor selection has to be driven by security features. Implementation of security features has to conform to the 802.16 standard that enforces AES-CCMP use for confidentiality.

WiMAX reliability is tightly bound to the quality of wireless planning and link budget calculations. Too tight link parameters can impact reliability of connection (e.g., in case of bad weather). Also, wireless communication can be affected by the lack of visibility between devices and can be disturbed by reflections. WiMAX introduction and its capabilities (e.g., advanced mesh architectures, support for quality of service) require a careful planning and design stage before deployment. The following are the key steps at this stage:

- Applications and services for WiMAX should first be identified. Next, traffic and protocol data flow models, and mobility requirements should be identified (WiMAX 802.16d does not support mobility unless combined with WiFi or other 3G technologies).
- Identify data and voice roaming needs – WiMAX to WiFi, CDMA, GSM, etc. Voice roaming may require IMS architecture.
- Develop end-to-end QoS strategy and QoS requirements for services and customers served. Insure management capabilities and procedures actively manage QoS
- Ensure existing strategy and policies can accommodate WiMAX additions.

- Spectrum analysis and busy frequency scanning in place of deployment are also important. Since wireless perpetrators are hidden and remote, it is easy to overlook dangerous situation or events going on in a wireless system.
- Special techniques are available to overcome the problem of ensuring visibility between devices and avoiding disturbance by reflections.

Wireless signal is susceptible to jamming and interference. Bad weather can have serious impact on badly designed wireless system when there is not enough link budget allocated for risk mitigation. Carefully conducted wireless budget planning can avoid network instability in bad weather (rain) conditions.

2.5. Cable Networks

2.5.1 Introduction

The availability and adoption of cable as an alternative medium to provide broadcast (analogue and digital TV) and communications services (Telephony and Internet) has been increasing throughout Europe, at a rapid pace, although not uniformly. In the last year, new cable companies have entered the European telecommunications market. Although cable deployment in the U.S. may be much more significant, we see the trend for more European cable penetration.

2.5.2 Usage and Market Trends

The penetration of cable services varies across the EU member states. TV services dominate the service penetration, followed by telephony and data. For TV services, Belgium and Netherlands lead the EU with over 90% penetration (of homes with TV), and UK and Spain lag behind, with about 10% penetration of TV homes[39]. However, Germany leads the EU in terms of gross cable user, standing at about 22 million subscribers, with over 55% penetration of TV homes. In total, there are about 64 million households in Europe that are served by Cable networks. This is about a third of households in Europe that have TV. The cable industry claims that cable can serve about 100 million homes today.

There are about 13 million households across Europe that are served by cable for telephony services. This number is expected to grow at an average of 30% per year over the next 5 years (see Figure 25)[40]. Cable telephony serves predominantly the residential market: Almost 91% of all cable lines in Europe serve the residential users, and only 9% serve the business customers.

39 http://www.cable-europe.eu/index.php?pid=43

40 Pyramid Western Europe Wireline market overview: Western Europe Fixed Communications Demand, June 2006

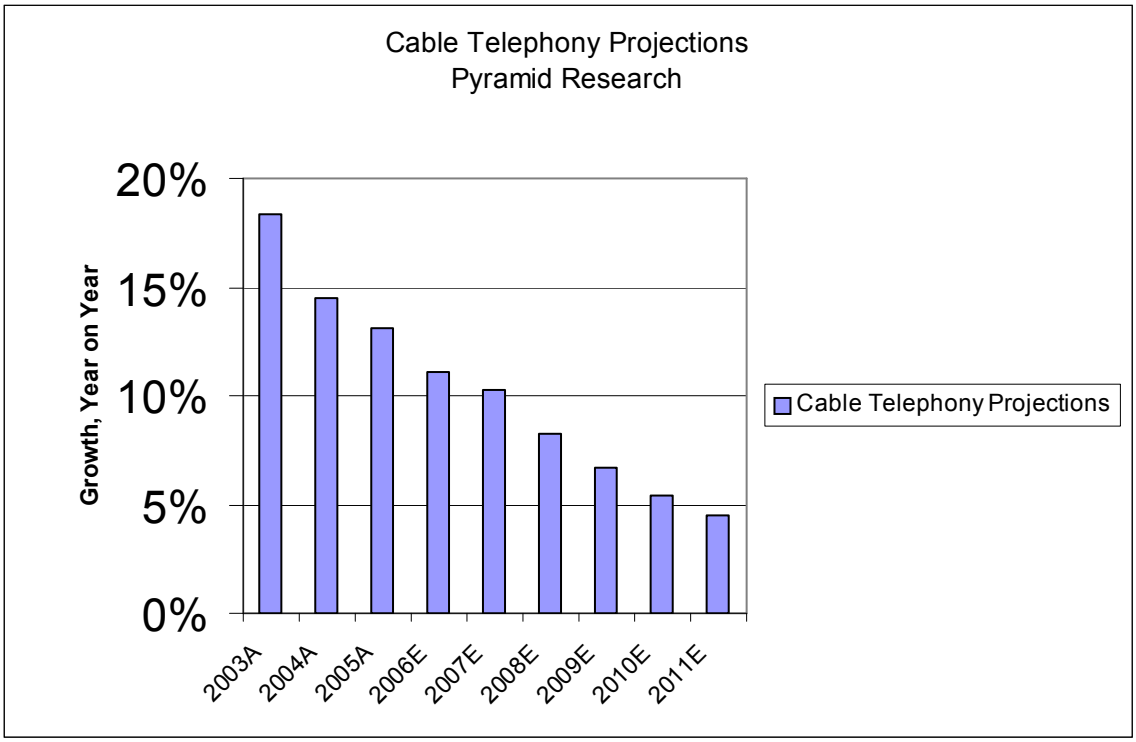


Figure 25: Cable telephony penetration projections (A=Actual, E=Estimate)

Cable networks also provide high-speed broadband Internet access, and serve a significant number of premises (residential and business) across Europe. At the end of 1Q06, there were about 10 million broadband cable Internet users in Europe, which is 16%[41] of total Broadband users in Europe. Cable based broadband access is growing at a rapid pace: Approximately 720 thousand broadband subscribers were added by the cable operators across Europe in 1Q06[42,43] (calculated by subtracting end-of-quarter subscribers for 4Q05 from 1Q06), which represents a strong 30% growth year on year.

2.5.3 Architecture of a Residential or Business Cable Network

To create high-speed Internet services, a cable operator creates a data network that operates over its Hybrid Fibre Coax (HFC) plant. The following diagram (see Figure 26) provides a high-level look at a typical large market cable network, including a Headend which feeds distribution hubs (each serving 20,000 to 40,000 homes) through a fibre ring. At the distribution hub, signals are modulated onto analogue carriers and then transported over fibre-optic lines to nodes serving 500 to 1,000 residential users. This fibre terminates in an optical amplifier and the signals are carried via coaxial cable over a distance of a few hundred to several thousand meters directly to the end user.

41 http://www.ectaportal.com/en/upload/File/Broadband%20Scorecards/Q106/FINAL%20BB%20ScQ106%20Press%20release%20Sept%2006.pdf

42 http://www.ectaportal.com/en/basic245.html

43 http://www.ectaportal.com/en/upload/File/Broadband%20Scorecards/Q405/Broadband%20Scorecard%20Q405.pdf

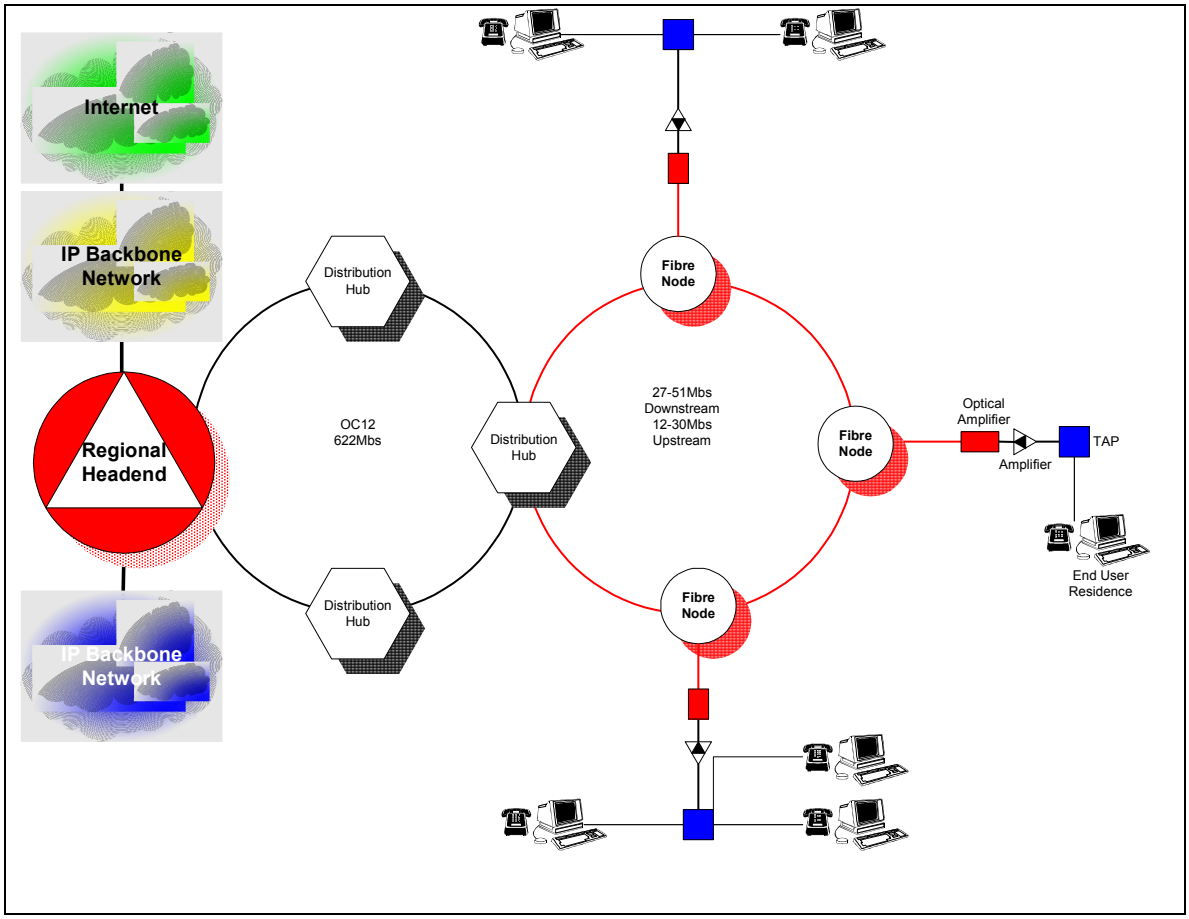


Figure 26: Cable delivery model from source to destination customer

With the emergence of Data Over Cable Service Internet Specifications (DOCSIS) and Euro-DOCSIS in the late 1990s, the HFC architecture is typically a star topology with the Coax acting as a form of Ethernet bus (shared bandwidth) topology. Users on the same frequencies on a Cable Modem Termination System (CMTS) port then share this upstream and downstream bandwidth. This star topology starts typically from the fibre node with runs of Single Mode Fibre (SMF). The target set by Euro-Cable Labs is to have no more than 500 residences being passed per node in order to offer a highly reliable and low maintenance data service. This is referred to as an “HFC-500”plant or architecture. Many cable operators do not achieve an HFC-500 since it requires significant investment. Europe is generally has HFC-1000 to HFC-6000 cable plants that service 1000 residences to 6000 residences.

Many cable operators in Europe are deploying high-capacity packet transport solutions over fibre rings connecting the CMTS units in their distribution hubs, such as Packet Over SONET (POS), at up to OC-12 speeds (622 Mbps).

2.5.4 Major Components of a Cable Network

- **CMTS:** A Cable Modem Termination System (CMTS) (see Figure 27) is the connection point at the Headend that terminates the radio frequency (RF) signal and converts the signal to data.

- **EMTA:** The Embedded Multimedia Terminal Adapter (EMTA) is a device that combines a DOCSIS cable modem and an analogue telephone adapter. The cable modem provides the data interface, and the telephone adapter provides the voice over IP (VoIP) interface for one or more analogue telephones. The terminal adapter provides the conversion between analogue voice signals and IP packets, delivers dial tone and manages the call setup.

- **Headend:** The video and data signals are collected and modulated at the Headend in a frequency stack known as the channel plan. This signal is sent to every home in the franchise area over fibre or coaxial cable.

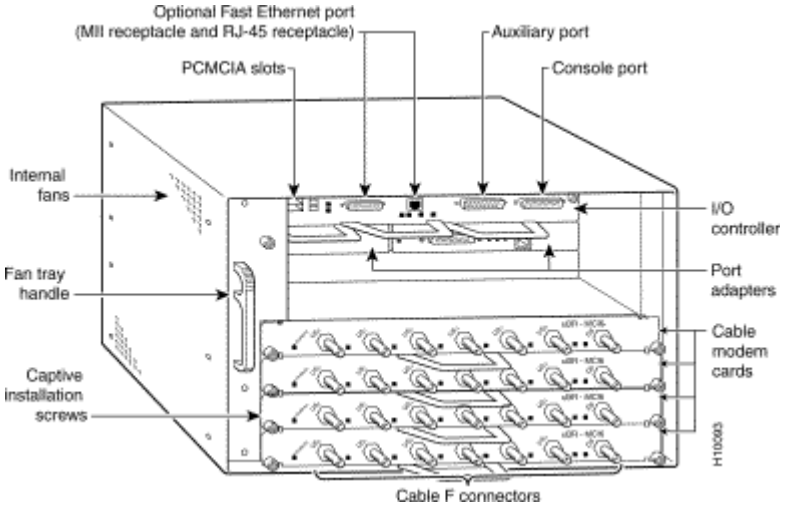


Figure 27: An example of a CMTS[44]

.

2.5.5 Brief description of the underlying technology

Cable Modem (CM), EMTA and set top box (STB) register on the network using the DOCSIS protocol. A configuration file is sent as part of the DOCSIS "handshake" that configures the communication parameters for the specific device. These modems are built by many companies (e.g., ARRIS, Motorola).

44 Shown in Figure 27 is the Cisco Systems UBR (Universal Broadband Router) 7246.

2.5.5.1 Registration

Registration begins with the CM or STB downloading a configuration file. The IP address of a configuration file server and the name of the configuration file the modem is to download are both included in the DHCP response to the modem.

The boxes (CM or STB) utilise the Trivial File Transfer Protocol (TFTP) to download the configuration file from the server. The configuration file contains information the modem or STB uses to operate, such as how much bandwidth it is allowed to use and which services it is allowed to provide. In the upstream "handshake" the service-provisioning items are set when the subscriber first calls in to request network service. This information is fed into an OSS to create the configuration file.

During the final phase of registration, the modem sends a registration message to the CMTS confirming the configuration file it received. The CMTS also retrieves a copy of the configuration file from the configuration file server. The CMTS using simple checksum checking compares the file from the server with the data from the modem to ensure the modem will only be using services for which it was authorised. Only after the configuration file data is verified is the modem finally allowed to transmit real user data onto the network.

2.5.5.2 DOCSIS Standard

The creation of a standard allows for cheaper manufacture of CMs and EMTAs. A primary goal of the creation of the DOCSIS standard was to move the cost of cable modems from more than €500 to less than €100 with a technology that was resistant to theft of service. DOCSIS accomplished those goals. This standard was created and is controlled by Cable Labs, which is funded by members of the cable industry worldwide.

The EuroDOCSIS standard was set up by a group of service providers to establish cross European standards. NTL, NetCologne, Telenet, Telewest, Casema, UPC NL, Essent, Tele Columbus and others have all signed up to this standard. A key benefit of EuroDOCSIS is the capability to use up stream frequencies up to 65 MHz rather than the DOCSIS 42 MHz cut-off. This provides a significant amount of relatively clean bandwidth in the upstream frequencies, which are a very critical resource.

2.5.6 Characteristics Regarding Cable Networks

A major challenge facing the cable industry is the investment required to add capacity as customers are added. This investment is primarily focused on "node splitting" which is adding fibre and CMTS ports. Increasingly customers are moving to more symmetrical data usage (Peer to Peer (P2P) file sharing, Gaming and VoIP) from what was initially an upstream to downstream data flow. The ratio of upstream to downstream data has changed from initially being 30:1 to now being closer to 2:1.

The cable industry has a long history of acquisition and consolidation. This results in a cable provider having a mix of hardware and software. The integration of the software between the provisioning systems and the billing systems is a constant and major challenge.

Cable industry also face continuing market challenges from Asymmetric Digital Subscriber Line (ADSL), Rate Adaptive Digital Subscriber Line (RDSL) and Broadband Digital Subscriber Line (BDSL) technologies and all are challenged by wireless technologies such as WIMAX. Broadband technology is now a commodity. Consumers are beginning to have more than one choice of broadband offerings available to them and will move to the service, which is the most competitive and reliable and meets the end users needs. The technology in use (e.g., whether ADSL or cable) will be less of an issue.

An “always on” connection that is available to the end user provides excellent ease of use but presents a security risk to the individual. The security risk can be reduced significantly through the use of either low cost cable routers, which provide Network Address Translation (NAT) or software firewalls. The DOCSIS protocol mitigates the risk of “theft of service” to the carrier. Additionally, DOCSIS provides the capability of link level encryption if the provider activates it.

A user who signs up for a relatively low bandwidth monthly account could “grab” or download “cloned” firmware of a user who is allowed faster service. Then “cloning” the MAC address, the malicious user populates the USB port so that to the upstream UBR it appears as if the malicious user is entitled to faster service and better connectivity. The service provider should implement integrated bandwidth management models that match level of service against DOCSIS configurations. Some companies have developed proprietary technologies that prevent such loss.

The final coaxial link to the home is bus architecture. The signals that go into one home also go into the homes that share connectivity to the “signal box” that are installed in neighbourhoods This is a major flaw in physical security (e.g., often these boxes with “taps” to homes are vandalised) and creates additional vulnerability by allowing a simple “network scanning” ability for any neighbouring user to use freely available tools to breach confidentiality.

The Headend sites in cable delivery architecture are often very poorly maintained due to fragmentation of companies and acquisitions during the 1990s. This means that often the Headend is a major weakness in the cable modem delivery model. Service providers should ensure regular maintenance of Headend sites.

The configuration file contains information the modem or STB uses to operate, such as how much bandwidth it is allowed to use and which services it is allowed to provide. The firmware resides on the cable modem or set top box and is often the subject of customer originated organised frauds.

Major malware infections (e.g., spyware, infected Windows PCs) originating from cable customers can cause loss of service or major capacity bottlenecks at DNS clusters at the network end. Typically a service provider allows his own customers only to query DNS. As the customers are white-listed[45], and rate limiting is not often an option, it causes service outages due to critical hardware and load balancers at the provider end becoming saturated. Network cleansing using either DNS or Cache technologies at network Headends or higher in the supplier network are required. Two market leaders for such products are Simplicita and Streamshield.

45 A whitelist is a list of valid addresses (e-mail or domain names) that a server is configured to accept.

It is not uncommon to find cable operators successfully providing data service on "old cable plants" (i.e. over 20 years old) with no fibre in place. Exposed coax can become antennas for noise produced by electric motors, radio transmitters and other common electrical devices. This noise is known as "Ingress". More that 80% of the noise is the result of the end user improperly adding devices (e.g., low-grade splitters to move or attach devices like television sets, games), poor quality cables and cables not properly tightened to the connectors. The cable providers can use external filters and filtered multimedia ports within the residence. Dynamic ingress blockers are also available. Implementation of DOCSIS and EuroDOCSIS 2.0 with Synchronous Code Division Multiple Access (SCDMA) allows operators to offer service in areas where noise has prevented the offering in the past.

2.6. Internet Core

2.6.1. Introduction

Internet access and usage is currently widely adopted in Western Europe and in the world. A majority of the users are using broadband (e.g., cable or xDSL) access services allowing them to enjoy high-speed access to the Internet. This, combined with a flat subscription fee, enables the introduction of new services like VoIP and IPTV to the customers.

While the access to Internet has been considered as a welcome development, the dependence on the Internet has also raised some issues, particularly due to the security aspects. One of the trends brought about by the Internet is the blurring of demarcation between the access and core communications networks, and the natural security the core network provides. Due to the ubiquitous nature of Internet Protocols, access to communications infrastructure is easier, which could result in malicious or accidental attacks resulting in economic impact on a country or the region as a whole.

2.6.2. Usage and Trends

Internet is widely used across Europe for information and communications purposes. The Internet penetration in the European Union is estimated at 50.3% of the total population of 462 million resulting in 22.3% of world's Internet users. This is about 32% more than the EU candidate counties as well as the rest of Europe[46].

There are several Internet Service Providers (ISPs) operating commercial Internet Autonomous systems across Europe. Internet Exchange is a physical infrastructure allowing many ISPs to exchange Internet traffic[47]. Traffic is exchanged by peering agreements made between the ISPs connected to the Internet Exchange. By peering at an Internet Exchange the connected ISPs reduce their reliance on a small number of networks (usually their upstream provider(s)), and this improves the delivery and receipt of traffic. This increase in efficiency benefits the connected ISP, and all its customers. The costs involved in connecting to an Internet Exchange are generally quite low for the improvement in performance that can be achieved. Most European Internet Exchanges are non-commercial co-operatives funded by membership fees paid by the connected ISPs, and are operated for the benefit of the member ISPs and the Internet community at large. Examples include the London Internet

46 http://www.internetworldstats.com/stats4.htm

47 http://www.euro-ix.net/glossary/

Exchange (LINX) and Amsterdam Internet Exchange (AMS-IX). There are at least 32 of these Internet exchanges operating across Europe[48].

Major trends that have been observed over the last decade include the move from narrowband to broadband Internet access with ~15% penetration in EU 15 (15 countries that were members of the EU before the enlargement on 1st May 2004), at end of 2005[49], driven mainly by user demands for improved experience and productivity. Internet is also heavily used for communications needs, supporting the messaging services like email and IM, as well as VoIP for peer-to-peer and public telephony services. The usage of VoIP has increased many folds in the last ten years. 1.8 million people use VoIP in the UK (7% of landline users) whereas, in Denmark, the VoIP minutes have superseded the PSTN/IN voice minutes[50].

Due to end-users being unsure about Internet performance, reliability security and robustness, many organisations and enterprises are now developing and using 'private' IP networks, instead of using the public Internet for the flow of sensitive and critical information. The Internet, however, also has characteristics which provide reliable and robust communications and organisations, enterprises and the public users do rely heavily on it. Thus, there is a debate over the relative availability and robustness of the Internet versus private IP networks. A few important facts showing this balance are listed in Table 3 [51]. It is important that the Recommendations in Section 4 apply equally well to the Internet.

Table 3: Characteristics of Public Internet and Private IP Networks

Characteristic	Public Internet	Private IP Networks
Underlying Facilities	Same private network facilities, but may not be managed with same time to restore	Private network facilities, with specified restoral SLAs
Interoperability and Trusted Network Entities[52]	Interoperability and trusted peering only assured at Internet exchanges, Network Access Points and Peering Points	Networks designed with interoperability and trust between all network elements and well as at Internet exchanges, Network Access Points and Peering Points
Network Access and Peering Points	Many; Specified SLAs	Private peering arrangements; Specified SLAs, Fewer than Internet
Topology	Highly meshed	Economically driven and much less meshed than Internet in general
User Access	Open to public; More opportunity for attack; same threats in general as private	More restricted access; more restricted opportunity for attacks, however, same threats

48 https://www.euro-ix.net/member/m/about/memberlist

49 EICTA BroadBand Scorecard: www.EICTA.org

50 www.morganstanley.com/institutional/techresearch/pdfs/Internet_Trends1005.pdf

51 A more thorough comparison may be found in "Next Generation Network Task Force, Appendix G," The President's National Security Telecommunications Advisory Committee, March 28, 2006

52 Particularly related to Recommendations 8 and 6

	networks	in general as Internet
User Authorisation	Lacking at network level; however non-consistently provided by many at applications level	Provided at network level; restricts users to appropriate network services and applications; Application level similar to Internet
Subscribers and Traffic	Non-deterministic; more unpredictable payload variations	Deterministic; easier to plan for end-to-end performance
Priority Services and Access[53]	Lacking; But vast capacity, mesh design and independence of legacy networks makes for availability during crises	Exists and expanding
Inventory of Critical Components[54]	Major peering and access points well known; Others not.	Well known

2.6.3. Architecture for the Internet

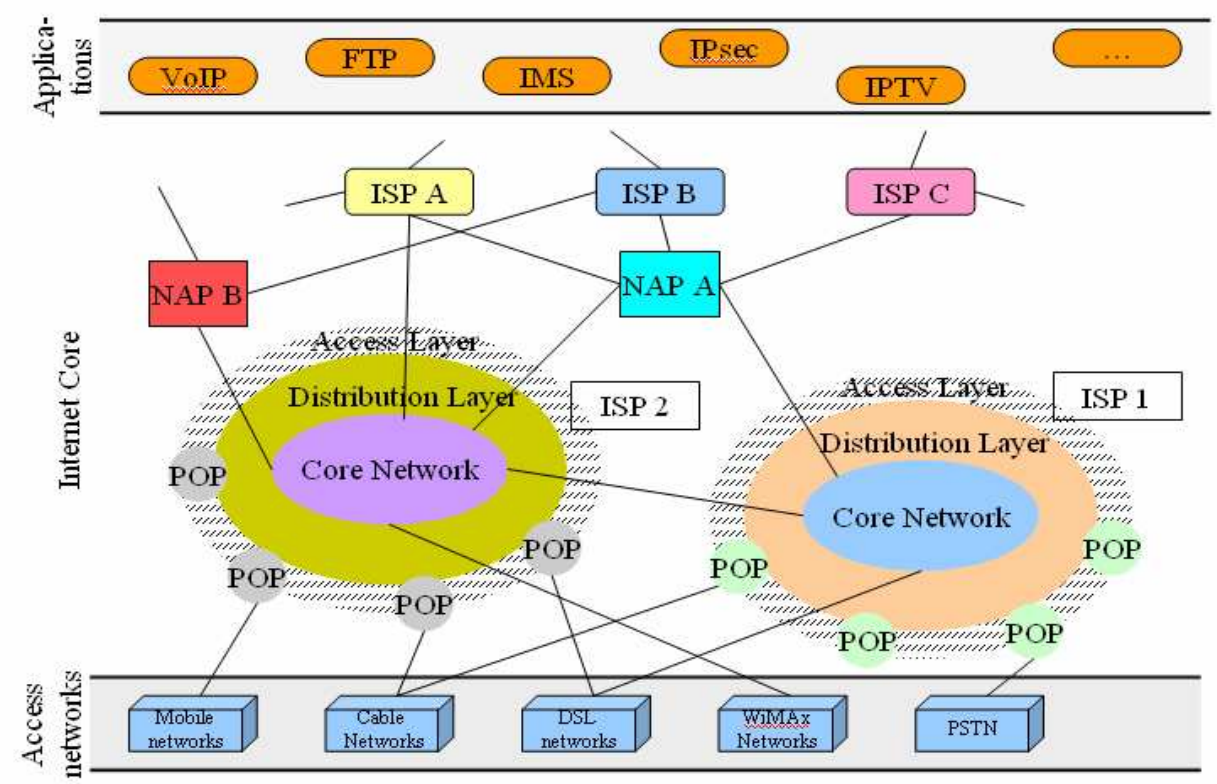


Figure 28: Architecture of the Internet

53 Particularly related to Recommendation 2

54 Particularly related to Recommendations 1 and 4

European ISPs use a hierarchical model for a design that simplifies the task required for internetworking (see Figure 28). A hierarchical network design includes the following three layers:

- The backbone (core) layer that provides optimal transport between sites. The core layer is a high-speed switching backbone and is designed to switch packets as fast as possible. This layer of the network should not perform packet manipulation since that would slow down the switching of packets.
- The distribution layer that provides policy-based connectivity. The distribution layer of the network is the demarcation point between the access and core layers. The purpose of this layer is to provide boundary definition and is the place at which packet manipulation can take place.
- The access layer that provides user access to the network. The access layer is the point at which local end users are allowed into the network.

2.6.3.1. Backbone

A backbone network is the top level of a hierarchical computer network. It connects to nodes at lower levels in the hierarchy. Backbone networks often exist solely to provide network connectivity between lower-level networks. In the early days of the Internet, a single backbone network existed in the form of the Advanced Research Projects Agency Network (ARPANET) and later, as the National Science Foundation Network (NSFNET). All other networks connected with one another via the Internet backbone, all routing information was conveyed between the backbone and the other networks via the Exterior Gateway Protocol. Today, there is no single backbone network for the Internet. Rather, each ISP has its own backbone network and exchanges traffic with other networks by peering or by transit agreements.

The Internet backbone refers to the main ‘trunk’ connections of the Internet. It is made up of a large collection of interconnected commercial, government, academic and other high-capacity data routes and routers that carry data across the countries, continents and oceans across the world. Part of the extreme resilience of the Internet is due to a high level of redundancy in the Internet backbone and the fact that the Internet Protocol routing decisions are made and updated in real-time during use.

2.6.3.2. Point of Presence (POP)

An Internet point of presence is an access point to the Internet. It is a physical location that house servers, routers, ATM switches and analogue call aggregators. It may be either part of the facilities of a telecommunications provider that the ISP rents or a location separate from the telecommunications provider. ISPs typically have multiple POPs, sometimes numbering in the thousands.

2.6.4. Major Components of the Internet

The components used in the Internet are the same as described in the other technologies and hence will not be described here separately.

2.6.5. Brief Description of the Underlying Technology

The ISPs are organised as Autonomous Systems (AS) to present a common routing policy to the Internet. A set of routing protocols that are used within an AS are referred to as Interior Gateway Protocols (IGP). The most used IGPs are Open Shortest Path First (OSPF) and Intermediate System to Intermediate System (IS-IS). To enable communication between their respective customers, one ISP exchange traffic with other ISPs via public peering points or via private peering agreements. To establish this routing between one another, ISPs are using the Border gateway protocol (BGP). BGP is used to exchange route information between Autonomous systems.

The main protocol used in the Internet Backbone is IPv4. IPv4 is a data-oriented protocol, best effort protocol that does not guarantee delivery. IPv4 provides unique global computer addressing to ensure that two computer over the Internet can uniquely identify one another. As the number of available IPv4 addresses is almost completely allocated, NAT is widely implemented. In the future, the IPv6 protocol that allows more addresses because of its longer address space, will replace the IPv4 protocol.

In order to meet the growing requirements in terms of performance and throughput, two mechanisms are currently widely used in the Internet backbone:

(i) MPLS is a data carrying mechanism which emulates some properties of a circuit switched network over a packet-switched network, and

(ii) Classless Inter Domain Routing (CIDR) that enables a significant reduction in the number of routes that have to be advertised over the Internet preventing 'routing table explosion' from overwhelming routers. CIDR also promotes the more efficient use of increasingly scare IPv4 addresses.

Besides the traditional purpose of the Internet (global exchange of data), more and more new services and concepts are being introduced based on the same underlying technology and network.

VoIP (voice over IP) is the routing of voice conversations over the Internet or through any other (closed) IP network.

IMS (IP Multimedia Subsystem) is a standardised Next Generation Networking (NGN) architecture for telecom operators that want to provide mobile and fixed multimedia services. It emerges the Internet with the cellular world: it uses cellular technologies to provide ubiquitous access and Internet technology to provide appealing services.

IPTV (Internet Protocol) TV describes a system where a digital television service is delivered using the Internet Protocol over a network infrastructure. It includes both live TV (multicasting) as well as stored video (Video On Demand or VOD).

2.6.6. Standard Bodies and Organisations

The Internet has no central operator but everyone operates a portion of the Internet. However, some central authority is required for the Internet to mange those things that only can be managed centrally (e.g., addressing, naming, protocol development). Among the significant Internet Authorities are:

- The **Internet Society (ISOC)**, chartered in 1992, is a non-governmental international organisation providing coordination for the Internet, and its internetworking technologies and applications. ISOC also provides oversight and communications for the Internet Activities Board.

- The **Internet Activities Board (IAB)** governs administrative and technical activities on the Internet.

- The **Internet Engineering Task Force (IETF)** is one of the two primary bodies of the IAB. The IETF's working groups have primary responsibility for the technical activities of the Internet, including writing specifications and protocols. The impact of these specifications is significant enough that ISO accredited the IETF as an international standards body at the end of 1994. RFCs 2028 and 2031 describe the organisations involved in the IETF standards process and the relationship between the IETF and ISOC, respectively, while RFC 2418 describes the IETF working group guidelines and procedures.

- The **Internet Engineering Steering Group (IESG)** is the other body of the IAB. The IESG provides direction to the IETF.

- The **Internet Research Task Force (IRTF)** comprises a number of long-term reassert groups, promoting research of importance to the evolution of the future Internet.

- The **Internet Engineering Planning Group (IEPG)** coordinates worldwide Internet operations. This group also assists ISPs to interoperate within the global Internet.

- The **Forum of Incident Response and Security Teams** is the coordinator of a number of Computer Emergency Response Teams (CERTs) representing many countries, governmental agencies, and ISPs throughout the world. Internet network security is greatly enhanced and facilitated by the Forum of Incident Response and Security Teams (FIRST) member organisations.

- The **World Wide Web Consortium (W3C)** is not an Internet administrative body, per se, but since October 1994 has taken a lead role in developing common protocols for the World Wide Web to promote its evolution and ensure its interoperability. W3C has more than 400 Member organisations internationally. The W3C, then, is leading the technical evolution of the Web, having already developed more than 20 technical specifications for the Web's infrastructure.

- The **Internet Assigned Numbers Authority (IANA)** is the entity that oversees the global IP address allocations, DNS root management and other Internet protocol assignments. It is managed by Internet Corporation for Assigned Names and Numbers (ICANN) through the IANA contract it has with the United States Department of Commerce.

- **Réseaux IP Européens Coordination Centre (RIPE)** Network Coordination Centre (NCC) is one of the four regional Internet registers that supply and administer IP addresses. Founded in 1989, RIPE NCC is a non-profit organisation. RIPE NCC provides IP numbers to Europe, the Middle East and parts of Africa and Asia. The RIPE community develops and set policies on the management and distribution of Internet resources (IP addresses and autonomous system (AS) numbers) through a long

established, open, bottom-up process of decision and consensus-based decision making. RIPE is a forum open to all parties with in interest in the technical development of the Internet in Europe. The RIPE community's objective is to ensure that the administrative and technical coordination necessary to maintain and develop the Internet continues.

2.6.7. Characteristics Regarding Internet Core

As the Internet continues to grow, the issues that confront its stable, beneficial evolution increase in number and complexity. On a high level, these threats can be categorised into several categories:

2.6.7.1. Security & Privacy

Due to the openness of the Internet, it has always been subject to attacks on the privacy and data of its users, by means of website hacking, e-mail spoofing, Distributed Denial-of-Service (DDoS) attacks, phishing, viruses, worms, Trojans etc. Over the last years the number of these attacks has increased spectacularly (see Figure 29).

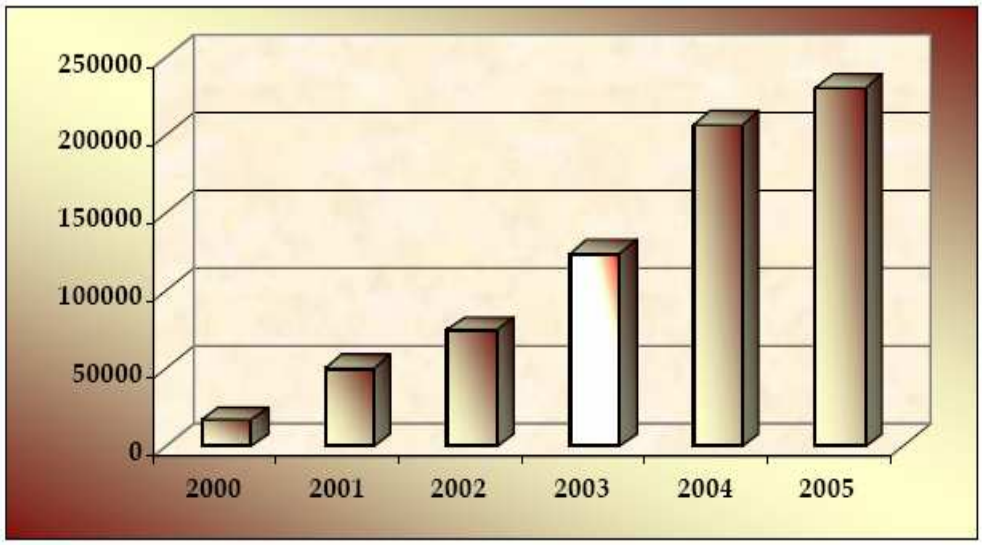


Figure 29: Yearly Comparison of Complaints Received via the IC3 website[55]

The complexity and global reach of the Internet has created an environment for the fast evolution of new generations of attacks, which are more sophisticated and therefore more difficult to detect. As these threats are evolving together with the technology, the attacks on the security and privacy will not disappear but will evolve into more complex and sophisticated forms. As such, they will remain a constant point of attention for the service providers. For example, "Blended Threats", such as Code Red and Nimda, are sophisticated attacks that are using multiple methods and techniques to propagate and inflict damage, thus

55 Internet Crime Complaint Center (IC3) 2005 Internet Crime Report. Note: Prepared by the National White Collar Crime Center and the Federal Bureau of Investigation.

spreading very rapidly and causing significant productivity disruptions. Blended Threats can be part virus, part worm and part backdoor.

2.6.7.2. Transformation to Future Networks

The era of separate networks for data, voice, and video is in the midst of a transformation that is converging on the Internet IP suite noted for its open architecture and also for the many threats that exploit its vulnerabilities for misuse. Transformation is never easy and with future networks, the complexity of this transformation must account for very different demands. The requirements of data packet transmission for email, for example, are not the same as those of voice transmissions where delays and session control are much more stringent.

The advent of next generation IP networks carrying converged voice and data traffic nullifies the inherent, built-in security of traditional telecommunications networks with their unintelligent end-user devices and out-of-band signalling and management networks. Now powerful, intelligent devices under end-user control are potentially able to access signalling and network management information. These powerful end-user devices are also subject to compromise and being used as platforms from which to launch DDoS attacks.

2.6.7.3. Quality of Service and IP Service Control

With the introduction of VoIP and IPTV services, latency and Quality of Service have become important aspects and selling points for service providers.

On the other hand, the growth of Peer-to-Peer traffic (P2P) traffic in recent years has been a growing problem for service providers. ISP do not generate any revenue from delivering P2P traffic to their subscribers, and smaller ISPs face considerable peering costs when P2P traffic inevitably goes off net. Even for ISPs large enough to not worry about peering costs, P2P drives increasing traffic loads, which requires additional capital expenditure for no additional revenue. Moreover, a minority of users generating large quantities of P2P traffic can degrade the broadband performance for the majority of subscribers using less intensive applications such as e-mail and web browsing. Poor network performance increase customer churn, which leads to a decline in service revenues.

With the advent of future networks comes the need for IP based service control, in order to have many different services running over a single universal IP network. A very significant aspect of this is that many of these services (such as VoIP or IPTV) need sophisticated performance guarantees (e.g., high security and low latency and jitter) and these have to be set up and controlled for each service instance, since the underlying general-purpose IP network does not offer them by default. In the past, service control has been single-service related, provided by the service supplier and locked into the service supplier's network equipment. As operators are moving to a future network approach with a single network supporting multiple services over multi-vendor network technology, they will be constrained by this silo approach to service control. ISP are looking into IP-service control solutions that can offer to them:

- Monitoring of network traffic to understand user- and application- level network use for troubleshooting, analysis and long-term planning
- Management of oversubscription to enable carriers to serve more subscribers over a given infrastructure

- Offer premium or new services to increase revenues, numbers of subscribers and ARPU
- Implement advanced billing models based on actual use of network services and reconciliation of network service offerings with subscribers' actual network usage
- Control and contain security threats to subscribers and the carrier network

2.6.7.4. Other Considerations

The popularity of the Internet has raised several non-technical but important social, legal and business issues. We describe some of them briefly.

Censorship and Freedom of Speech
The Internet raises issues of censorship and freedom of speech. Should governments or other institutions be able to censor the content available on the Internet or does this interfere with individual rights? With people from different countries, cultures and of all ages on the Internet, should there be consideration of what is appropriate for everyone?

Internet Business
The Internet is one of the newest and fastest growing markets. Advertising, electronic commerce, online banking and online gaming have raised debate about the future economy. How is business evolving to target the online community and to meet the demands of new technologies?

Laws & Regulations
The Internet has forced us to examine how the laws apply in cyberspace. With an increasingly growing and diverse population of Internet users it is inevitable that some information may be inappropriate for certain people. The discussion on what is appropriate and what should be regulated on the Internet is raging across different groups: parents consider filtering software, governments debate laws about online pornography, artists and web designers consider digital copyright.

2.7. IP Networks

2.7.1. Introduction

A big attraction of future networks is their ability to support multimedia services. Recognizing that IP networks are basic to future networks, this section provides background on the architecture of IP Networks to support multimedia services. Depending on the context, the term “IP network” will refer to the core IP network or access IP network or LAN.

2.7.2. Architecture of IP Networks

An IP network(s) supporting VoIP services with different access arrangements is shown below (see Figure 30).

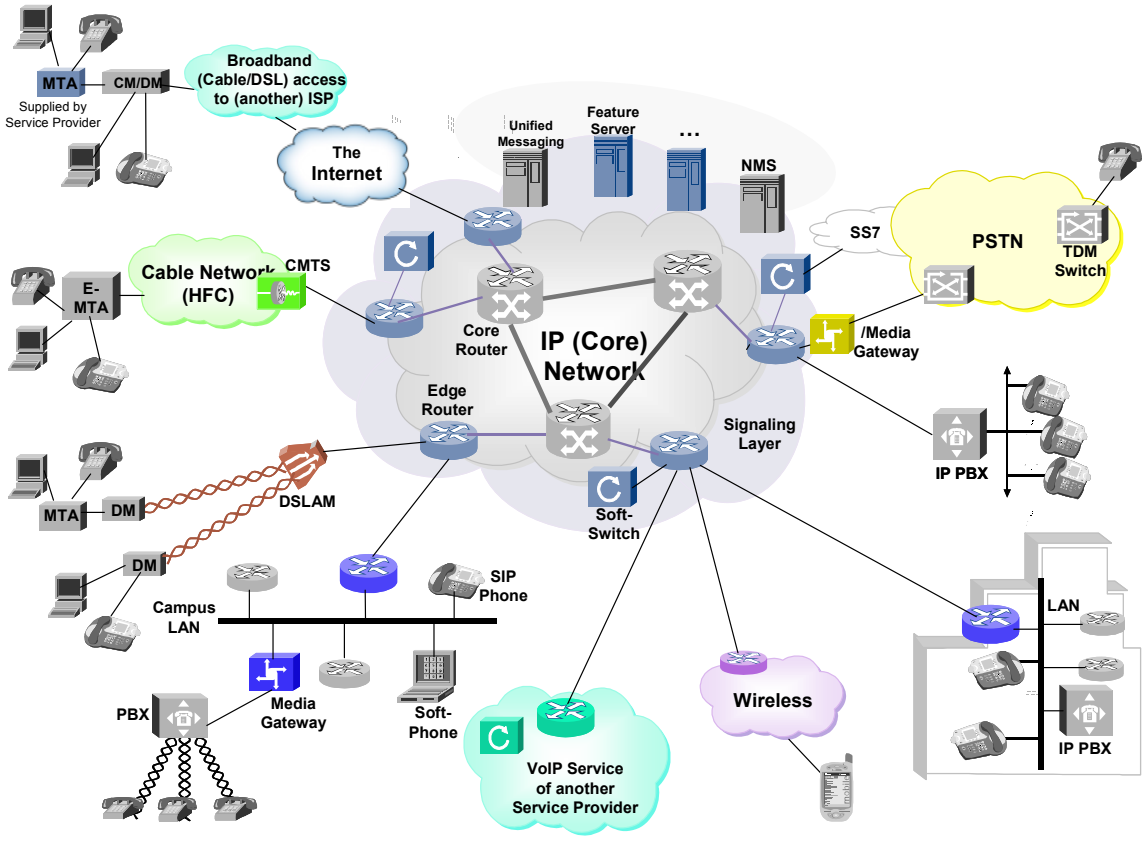


Figure 30: An Example of IP network technology supporting VoIP service

Note that in this example illustration, many access arrangements such as the HFC access, DSL access can themselves be an IP network connecting many CMTSs and DSLAMs, respectively.

2.7.2.1. LAN Architecture

A location (customer or data centre) connecting to the IP core network may consist of an IP host or the location may be a LAN of many hosts, IP switches and routers. Some of the examples of host are SIP phone, Internet Access Device (IAD), gateways, multimedia servers, and SBCs as shown below for a VoIP "Telephony Office LAN (see Figure 31)."

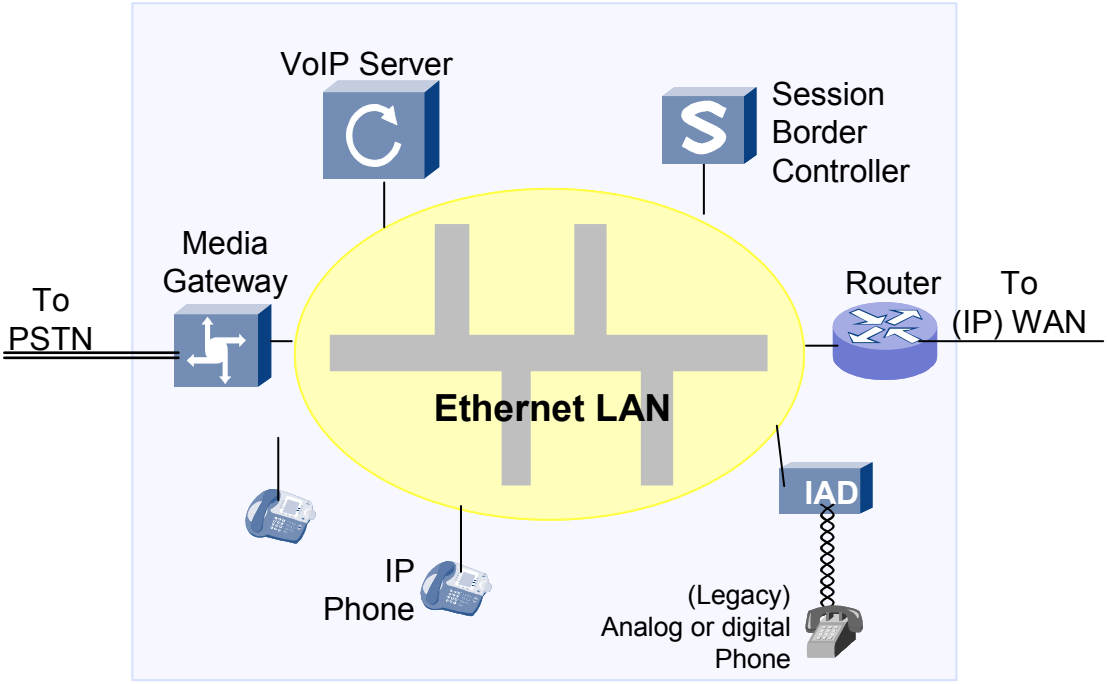


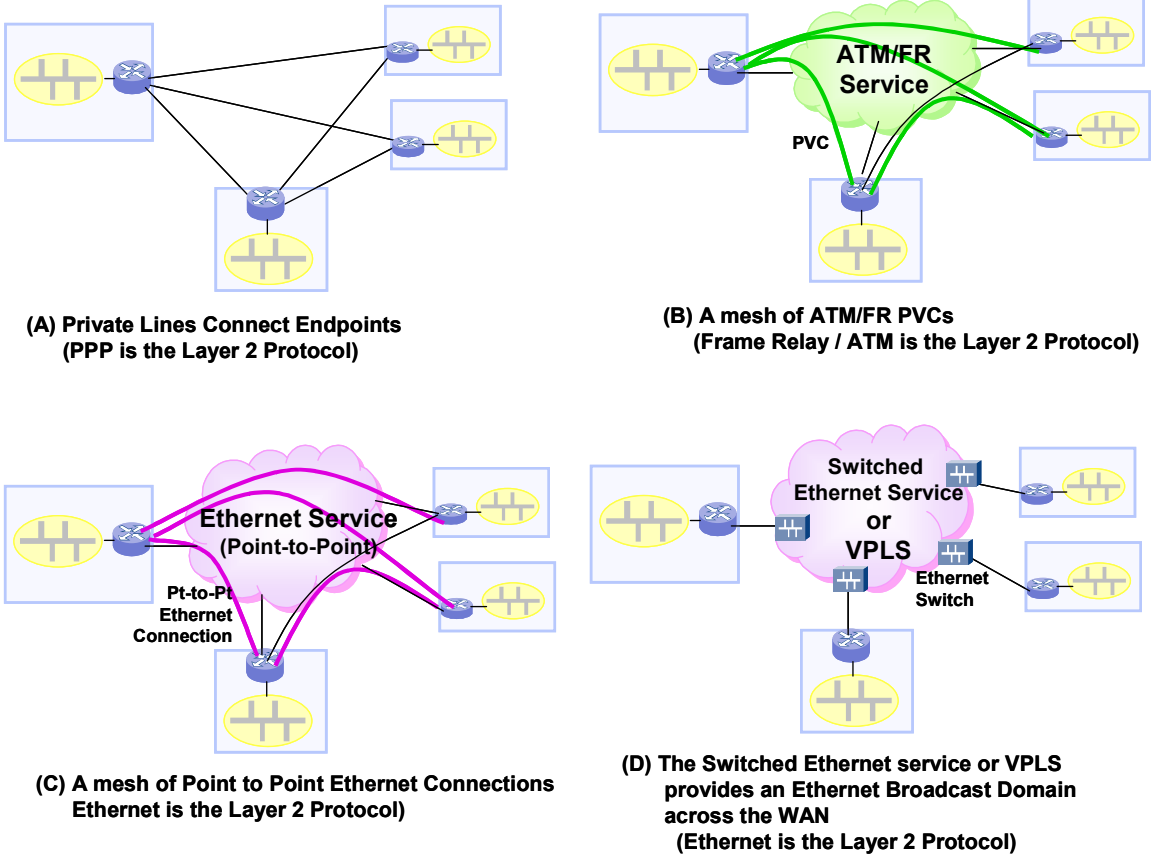
Figure 31: An Example of a LAN

Even though many other LAN technologies have been used is the past, most LANs today are based on the Ethernet technology deployed through interconnection of Ethernet switches and hubs in a building or over a campus of buildings. One or more routers connect the LAN to the IP WAN.

2.7.2.2. WAN Interconnection Architecture Options

IP WANs connecting the endpoints (i.e. individual IP hosts or IP routers connecting the LAN to the WAN) fall into two basic categories:

In category 1 the WAN provides Layer 2 (OSI model) connectivity between the end points (see Figure 32 that shows the four most common scenarios in Figures 32(A) through Figure 32(D)).



(A) Private Lines Connect Endpoints (PPP is the Layer 2 Protocol)

(B) A mesh of ATM/FR PVCs (Frame Relay / ATM is the Layer 2 Protocol)

(C) A mesh of Point to Point Ethernet Connections Ethernet is the Layer 2 Protocol)

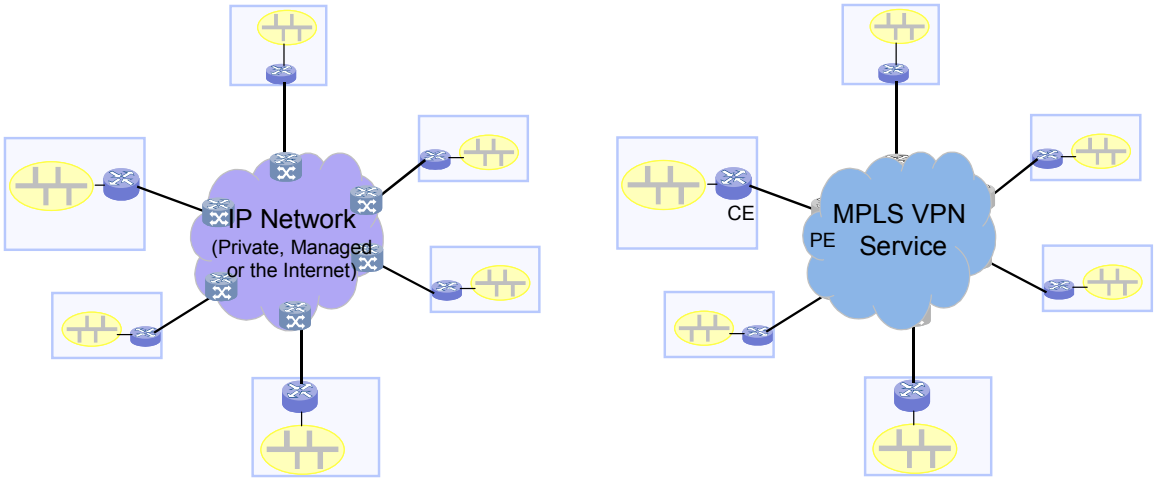
(D) The Switched Ethernet service or VPLS provides an Ethernet Broadcast Domain across the WAN (Ethernet is the Layer 2 Protocol)

Figure 32: IP network connects End points over Layer 2 Network Technologies

- Figure 32(A): A mesh of private lines connects the endpoints. This is a viable option if the number of endpoints is very small or the IP infrastructure is considered private and extremely secure. IP connectivity between the endpoint routers uses PPP (Point to Point) as the Layer 2 protocol.
- Figure 32(B): The connectivity is over ATM/Frame Relay service. IP connectivity between the endpoint routers uses ATM/FR as the Layer 2 protocol across each Permanent Virtual Circuit (PVC) in the mesh of PVCs.
- Figure 32(C): Lately, many service providers offer Ethernet connectivity. A mesh of point-to-point Ethernet connections between the endpoint routers provides the IP connectivity between the endpoint routers. Thus, Ethernet is the Layer 2 protocol between the routers.
- Figure 32(D): If the Ethernet service is a switched Ethernet service including the new Virtual Private LAN Service (VPLS) service, all endpoints can consider themselves as being on a single Ethernet even if they are at different locations. Thus, every pair of endpoint routers has an Ethernet connection between them (any to any connectivity). Once again, Ethernet is the Layer 2 protocol between the routers.

With Layer 2 connectivity all IP connectivity is the responsibility of the organisation(s) that connect into the Layer 2 network. This includes routing, peering, QoS, and IP performance. Thus, this Layer 2 option is not very attractive when the endpoints are owned by multiple organisations including individual customers.

In category 2 the WAN itself is an IP network of routers (see Figure 33 that shows the two most common scenarios in Figures 33(A) and 33(B)).



(A) IP Core with Native IP Service

(B) IP Core MPLS VPN Service

Figure 33: IP network connects End points over Layer 3 Network Technologies

- Figure 33(A): The IP network may be the Internet itself, or a managed IP service from an ISP, or a private IP infrastructure.
- Figure 33(B): The IP network is really a VPN subscribed from an MPLS VPN service of an ISP. MPLS VPNs service is defined in RFC 4364 (which replaced the well known RFC 2547).

In either case, the endpoint router connects to the IP network router over a Layer 2 connection. (Note that this access L2 connection itself could take one of the four forms defined in Figure 32). For the MPLS VPN service, the endpoint router and the IP network routers are respectively called customer edge (CE) and provider edge (PE).

Routing protocols such as BGP must be used between endpoint router and the connecting IP network router. Other routing protocols such as RIP and OSPF are also possible, though not common.

2.7.3. Brief Description of Underlying Technology

Only those IP networking items are discussed here that have relevance to the issues listed in the next section.

2.7.3.1. IP Addressing

IP networking of today is based on version 4 (IPv4) addressing scheme of 32-bit IP address for any IP addressable system (e.g., server, router, IP phone). IP addresses are globally unique and these “public” addresses must be obtained from IANA-designated authorities such as Reseaux IP Europeans (RIPE).

A small portion of IP addressing space is considered “private” addressing space as defined in RFC 1918. Private addressing may be used within a private network that does not have direct IP connectivity to outside networks. Endpoints in a VPN including MPLS VPN may use private addressing.

A NAT-capable router can provide connectivity to private addressed endpoints on a LAN to connect to outside (e.g., the Internet) through the router.

Introduction of IPv6 will allow for increasing the IP addressing space to 128-bit addressing and more efficient implementation of QoS capabilities.

2.7.3.2. Tunnelling

A tunnel is a logical path through the IP network connecting two endpoints. Tunnel traffic passes transparently through the IP network; for example, private addressing can be used between the endpoints.

VPNs use tunnelling as the basic mechanism. A mesh of IPSec tunnels among the endpoints helps configure a secure VPN across the Internet. RFC 4364 provides for generalised VPN with any-to-any connectivity using tunneling through an IP network. MPLS VPN service is the most common RFC 4364-based service today that uses MPLS Label Switched Paths (LSPs) as the tunneling technology. Note that a VPN can use private addressing even if the tunnels may be carried over the network that also carries the Internet traffic and traffic for multiple VPNs.

Additionally, MPLS LSPs provide for security of an ISP’s core network by not distributing the Internet and customer routes to the core routers.

2.7.3.3. Quality of Service

To meet customer expectations of any multi-media services delivered over the IP network, the IP network must implement QoS. Media quality – voice quality and video quality – depend on many factors including the IP network performance. Quantitative metrics such as Mean Opinion Score (MOS) have been widely accepted as a measure of voice quality and models and tools are available for measuring MOS of a VoIP call. Similar activities are underway in definition and measurements of video quality. Voice and or video quality are affected by the network delay, jitter and packet loss in the IP network. Certain buffering techniques and clever algorithms in the end systems (such as IP phone) can correct for some amount of jitter and packet loss in the network; however, it is extremely important that the IP network resource allocation must minimise delay, jitter, and packet loss in the network.

Generally, priority treatment to the voice and video traffic in the IP network over other data traffic including the “best effort” traffic will reduce these three impairments resulting in better media quality. Also, even the signalling traffic must be given priority to reduce network delays to keep the call set up times within acceptable limits.

There are two approaches to QoS to support multimedia applications including voice and video. In the Integrated Services (IntServ) approach to QoS, end-to-end network resources are allocated individually to VoIP connections in either direction using the Reservation Protocol (RSVP) (-like) signalling protocol for preferential treatment to the voice traffic resulting in bounded values for latency, jitter and packet loss. Even if physical resources in

the network including links are shared between VoIP and data traffic, there is guaranteed bandwidth (and other resources) provided to the VoIP end-to-end.

However, IntServ requires a high processing load in the routers and is not very scalable with the current technology for per call signalling. Tunnelling technologies such as MPLS LSPs can be used to manage these flows with RSVP-TE used to create tunnels and for maintaining their rerouting. But, in that case, resource reservation requests can be few and far between. Using IntServ for VoIP QoS requires frequent creations and destruction of "voice" tunnels.

The Differentiated Services (DiffServ) is perhaps the most prevalent approach to QoS implementation in IP networks. The DiffServ model renders each packet a QoS treatment based on the class of service of that packet at each hop through the network – the specific Per-Hop-Behavior (PHB[56]) is specified and configured at each router instead of the end-to-end resource reservation of the IntServ model. Most vendors of routers and switches support DiffServ model and many IP service providers support QoS treatment for several classes of service such as voice, video, critical business data, etc.

A mapping of QoS classes to typical traffic class treatment used by IP networks is shown below (see Figure 34).

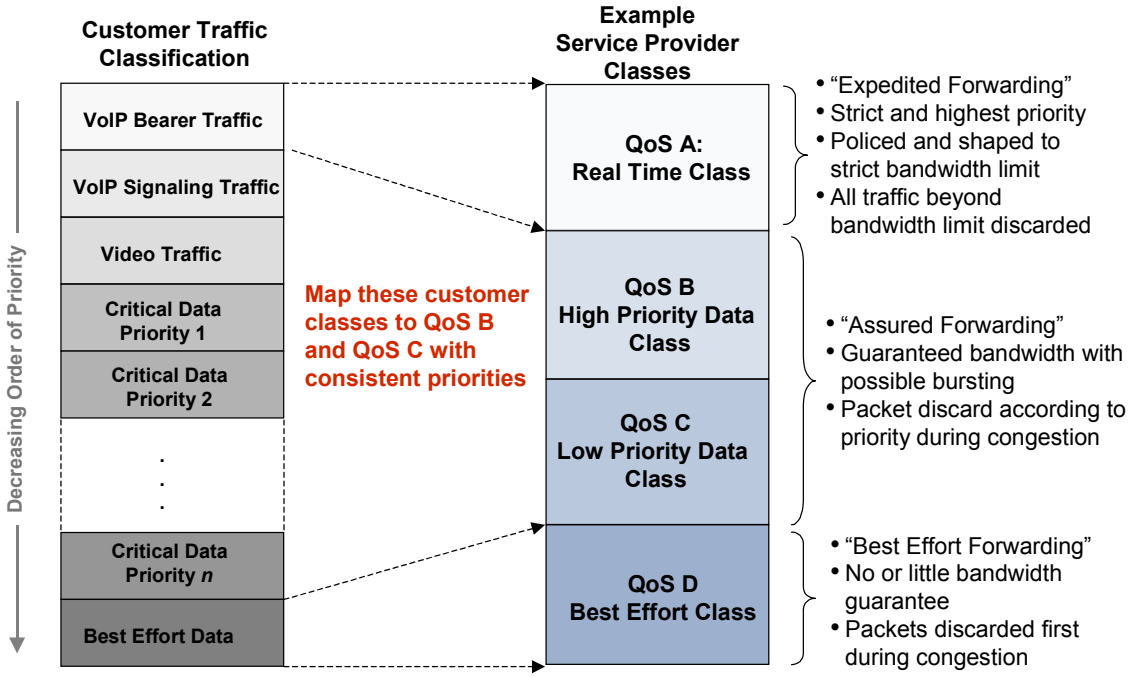


Figure 34: QoS with DiffServ – Example Mapping of Traffic Classes

Typically, an IP service provider would support a strict priority class for real time traffic such as VoIP bearer traffic, one or two traffic classes off varying priority, and a best effort class of lowest priority.

56 When packets are classified at the edge of the network, specific forwarding treatments, formally called Per-Hop Behaviour (PHB), are applied on each network element, providing the packet the appropriate delay-bound, jitter-bound, bandwidth, etc. This combination of packet marking and well-defined PHBs results in a scalable QoS solution for any given packet, and any application.

Important characteristics of the PHB for these classes are listed in Table 4 below.

Packet classification is signalled by the values in the corresponding field in the packet header. Examples of these "QoS fields" are TOS or DSCP in IP header, EXP in MPLS header, and IEEE 802.1p in an Ethernet header.

Even with network QoS, if the traffic demand for multimedia sessions (e.g., VoIP calls) exceeds the designed network capacity, the increased demand affects all existing calls, not just the new calls exceeding the demand. Therefore, it may be prudent to exercise a centralised control that will block new calls based on the dynamic network conditions, so that, the existing calls can receive required resources for their media quality objectives.

There has been little support for such central control in most IP network based multimedia services to date with PacketCable based VoIP service being one notable exception[57]. Lately, there has been considerable activity in developing related product features and standards development.

RACF consists of the central PD-FE (policy decision functional entity) that is responsible for determining the resource management policy as a function of the network condition, and the transport resource control functional entity (TRC-FE) that is responsible for collecting the network measurement statistics from the edge and core routers periodically. PD-FE periodically communicates the current call admission policy to the Policy Enforcement Functional Entity (PE-FE) in the access network. PE-FE implements the call admission control for the incoming calls.

2.7.4. Other Considerations in IP Networking

IP networks have evolved in providing robust transport mechanisms for carrying voice and other multimedia applications with the performance, quality, and availability expectations based on past experience and promise of reduction in total cost of ownership. This section discusses other considerations in IP networking as a converged network for carrying multimedia applications.

2.7.4.1. Networking Technologies

Network Architecture: Given the variety of network architectures, which is the right one to choose for ensuring reliable and secure communications? This is important not only when a new IP network infrastructure is created for migrating the multimedia services from their legacy networks, but also for deciding on architectural changes that may be necessary while introducing new multimedia applications on an existing IP infrastructure.

Table 4 below provides a summary of the relative benefits and drawbacks of the many IP networking architecture options described in Section 3.2.2 with the important considerations in their selection.

57 PacketCable VoIP specifications use the DOCSIS QoS of defining service flows that are specific to VoIP calls. Thus, if the capacity used by the service flows for the existing VoIP calls exceed the available HFC bandwidth, new incoming calls are blocked.

Architecture Type	Benefits		Drawbacks	
Figure 32(A): Interconnection with point to point private lines	1. Totally secure and private if not connected to outside networks	1. Good for hub-spoke types of applications 2. More secure, in shared networks, since no IP access to the network elements (e.g., from the outside)	1. Costs may be prohibitive if connecting more than a handful of sites	1. IP network operation including inter-location connectivity is the responsibility of the end-points. 2. Without full mesh connectivity, IP traffic may hop from location to location. 3. Cannot directly connect to other IP networks – need peering at an endpoint locations
Figure 32(B): FR and ATM Service	1. Perhaps the most prevalent and available L2 technology		1. Full mesh of connectivity can be expensive 2. Giving way to Ethernet and MPLS VPN technologies	
Figure 32(C): Ethernet service with point to point connections	1. Probably more cost effective with very high data rates 2. Same L2 protocol for LAN and WAN connectivity		1. Full mesh of connectivity can be expensive 2. May not be available except in a metro area	
Figure 32(D): Switched Ethernet service and VPLS	1. Probably more cost effective with very high data rates 2. Same L2 protocol for LAN and WAN connectivity	1. Any-to-any L2 connectivity. Do not need to define point to point connections	1. Service may not be available except in a metro area 2. *Perception* that Switched Ethernet is less secure (Mostly mitigated by using customer-specific VLANs and VLAN stacking)	
Figure 33(A): IP network with native IP connectivity	1. Most prevalent and available. Internet is always there. Many ISPs offer managed IP services with enhanced options for reliability and security1. 2. Any-to-any IP connectivity 3. IP service responsible for all IP-related operations including routing between locations 4. IPSec tunnels can be used for defining secure VPNs - ideal for hub-spoke style connectivity when MPLS VPN is not practical.		1. The Internet does not necessarily provide reliability, security, and QoS unless managed IP services are used.	

Architecture Type	Benefits	Drawbacks
Figure 33(B): MPLS VPN service	1. IP service responsible for all IP-related operations including routing between locations 2. A cost-effect private networking over shared networking resources 3. More secure with private addressing and no IP connectivity to outside of the VPN 4. Generally, no need for additional function for the endpoint routers (CE) 5. More flexible than the VPNs based on point to point IPSec tunnelling	1. Can be more expensive than native IP service 2. Difficult to interconnect to other VPNs or Internet even for applications such as VoIP to connect to the outside world. (But, SBCs can help bridge traffic between different domains – the *pinhole* capability) 3. Perception of not being very secure and stable when MPLS services are carried over the ISP networks that also carry the Internet traffic (Mostly mitigated if the service provider separate PEs from other edge routers and remove Internet and other customer routes from the core routers)

Table 4: Summary of Benefits and Drawbacks of IP solutions

IPV6: The main improvement brought by IPv6 is the increase in the number of addresses available for networked devices and the solution of the IPv4 address space exhaustion problem. End-to-end IP connectivity often requires traversing through IP networks of different providers who may deploy router products with varying versions of IP leading to interoperability problems.

Vendor products supporting IPv6 may not support full IPv4 capabilities. There will be a definite, perhaps slow, migration to IPv6 over time. Therefore, subject to cost considerations, it is prudent to procure and deploy IP networking systems that will support IPv6 when needed. It should be noted that IPv6 endpoints could always connect over a tunnel through an IPv4 network.

Private Addressing: Customers, including residential and small businesses, want to use their own private addressing on the systems connected on their LAN. This enhances security, as the customer does not have to expose their systems to the outside world. It also reduces the number of IP address required from the service providers' pool of IP addresses.

Most routers, including those used at home LANs support NAT. For VoIP applications, use of a customer location-based SBC must also be considered. SBC do provide NAT functions. Thus, for connecting the LAN to the outside world only the particular router or SBC need to have an IP address from the service provider pool of IP addresses. If the firewall functions are also built into the router or SBC, the customer will be able to provide isolation of its endpoints from outside and still offer the connectivity to the multimedia services as needed.

Access to Servers: The multimedia server locations (e.g., Telephony Office) contain many servers and other systems connected into the LAN, possibly using their own addressing system. Customers of the service need direct access to some of these systems. Even if the IP addressing of these systems uses public addressing, the service provider may not want to advertise these IP addresses widely. Providing only one IP address for the service is a good business practice and separation of addressing space has added security advantages.

An approach is to deploy SBC at the location that connects into the LAN of the servers and only make the SBC IP address known to the customers. In addition to NAT function, the SBCs can support deep packet inspection to intelligently guide traffic between the required servers and the customers.

2.7.4.2. Quality of Service (QoS)

Core QoS: Though an IP network service provider may offer QoS, end-to-end delay jitter and packet loss may still be unacceptable to the end users. This could be because many IP service providers implement QoS only at the edge of the network and not within the core network. Such service providers assume that there is excess bandwidth (resources) inside the network and that QoS is needed only at the edge since the access links have limited bandwidth. This assumption is not necessarily valid unless the link utilisation within the core is very small. Even for moderate link utilisation, without QoS, the multimedia traffic will experience excessive jitter.

It is important that the IP service provider provides SLAs on end-to-end delay, jitter, and packet loss and is held responsible for delivering on these SLAs. In some cases, increasing bandwidth may be necessary for the IP service provider if QoS implementation in the core fails to meet the SLAs. It is always a good practice that the multimedia services implement adequate jitter buffering, and possibly packet loss concealment algorithms, in the end systems such as the gateways and IP phones to compensate for some jitter and packet loss in spite of QoS in the network.

Central Controls: In spite of diligent QoS implementation and network design, QoS problems do come up, particularly when there is a marked increase in the demand. Without a centralised call admission control, there is no limit to the number of multimedia calls admitted to the network increasing the corresponding traffic beyond the designed capacity. The traffic for calls admitted beyond the designed capacity, affect traffic for *all* existing call and not just the new calls. Even if strict priority QoS is implemented for real time traffic, the policing and scheduling of the real time traffic will discard packets that exceed the designed bandwidth, resulting in packet loss for all calls.

A centralised call admission control that is based on limiting the number of calls (sessions) could be implemented. These techniques are being worked at this time. Call admission control does imply blocking of certain amount of customer demand. An optimal solution will maintain the required voice quality–related networking parameter (e.g., based on packet loss) subject to a maximum acceptable blocking probability.

Peer-to-Peer Traffic: There is considerable peer-to-peer traffic (e.g., Bit Torrent) in the IP network that could affect the quality of the multi-media traffic.

QoS treatment for the multimedia traffic should alleviate the problem. There are products that can isolate the peer-to-peer traffic and the IP service provider can determine the ways to handle such traffic for overall satisfaction of all customers. It should be pointed out that MPLS is not necessary for QoS.

Voice Quality: There are situations when voice quality measurement tools report good voice quality (i.e. Mean Opinion Score, MOS greater than 4), but customers still report voice quality problems.

Most VoIP quality measurement tools calculate MOS based only on measurement of networking parameters such as delay, jitter, and packet loss. Some others report only on listening quality and not on conversational quality. If there are little network related impairments due to QoS implementation, MOS score may seem acceptable. But voice quality experienced by users depends on many other factors such as background noise, signal levels, and echo. These impairments occur outside of the IP network. Network delays such as echo can exacerbate some of these impairments. It may not be possible to reduce network delay, particularly if QoS is effective. for a solution could be to increase the tail of the echo canceller in the media gateways, if possible.

3. Reliability Considerations Common to Future Networks

Section 2 discussed reliability pertaining to specific future network technologies. This section addresses reliability common to all of the technologies. They apply to Europe's future communications networks and to other networks around the world. The discussion will include:

- Design Methodology
  - Metrics and Requirements
  - Complexity
- Network Operations
  - Reliable Network Operations
  - Procedural Reliability
- Network Resource Management
- Impact of Security Vulnerabilities
- High Degree of Interconnection

Each of these is in varying stages of being addressed by the industry.

3.1. Design Methodology

The future networks are much more multi-technology networks than the legacy networks and offer multiple services and applications that stress the network differently. At least two aspects are required for a good design of these networks: 1) the set of network reliability metrics and objectives that the design will target; and, 2) the design methodology itself.

3.1.1. Metrics and Requirements

3.1.1.1. End-to End Requirements for Design of Network Reliability

The future networks will be multi-services networks that will support a variety of new services and applications. Many of the reliability metrics for these multiple applications and services, as well as the corresponding end-to-end objectives are not yet defined. of the setting of appropriate requirements can ensure controlled capital expenditures, for the network operator, and appropriate end-user service reliability expectations. When network operators or service providers are not necessarily clear on the reliability metrics and requirements needed, they sometimes revert to the PSTN/IN availability objectives (i.e. "5-9s") for all applications. Each application, however, has very specific characteristics (e.g., always on,

location and presence, real time, store and forward, throughput) that stress the network differently. Thus, each application type will have its own metrics and requirements.

3.1.1.2. Standards-based Equipment Reliability Requirements

Examples of standards-based reliability equipment requirements to be specified are

1. Signalling Gateways (SG) or Media Gateway Control Functions (MGCF): The signalling traffic to and from the PSTN/IN traverses the SG or MGCF. These are new elements that carry a high volume of calls.
2. HLR/HSS: The HLR/HSS is an element in 3G and new IP networks that contains an enormous quantity of all end-user location, profile, account, and other data essential for network service.

3.1.1.3. Competing Standards

Where standards do exist for future networks, there are sometimes overlapping standards, developed by different standards organisations that need to be reconciled. An example includes VoIP reliability. Published objectives from two organisations exist: the CableLabs Objective[58] and ATIS Objective[59]. Table 1 shows the very different reliability requirements.

Table 5: VoIP Objectives Differ by Standards Organisation

End-End VoIP Service Reliability Metric	CableLabs Objective	ATIS Objective**
Downtime	< 315.36 min/yr	< 15.00 min/yr
Availability	> 99.940%	> 99.997%
Expected Cutoffs	1.25 per 10,000 calls Pr{Cutoff} = 0.000125	0.35 per 10,000 calls Pr{Cutoff} = 0.000035
Expected Ineffective Attempts	5 per 10,000 calls Pr{Ineffective Attempt} = 0.000500	

Once the set of accepted metrics and objectives are specified network operators will deliver consistent reliable service based on of the proper objectives, thus minimizing confusion and, potential, dissatisfaction for the consumer.

3.1.2. Future Networks Reliability Design Methodology

Future networks need new network reliability design methodologies. The networks will be very dynamic (e.g., wireless access will transfer between WiFi, WiMAX, and 3G), will have

58 PacketCable (http://www.packetcable.com) Requirements (Pkt-tr-voipar-v01-001128)

59 Standard on Reliability-Related Requirements, Metrics and Terminology for Network Solutions – US Alliance for Telecommunications Industry Solution (http://www.atis.org/) Performance, Reliability, and Quality of Service Committee (PRQC), PRSSC – T1A1.2/2003-148, Appendix B.

disaggregated and geographically distributed network functions that use multiple databases, application servers, and gateways, and, will be connection and connectionless oriented. Existing methods will be inadequate to deal with these complexities.

3.1.2.1. Multiple Reference Connections for Reliability Design

One or two reference network connections are usually sufficient for representing the legacy network reliability models. This is true because they usually support a small number of applications and the applications usually involve a limited number of call and data functional entities. This is no longer true for the future networks. Their disaggregated implementation of network functionality, multi-services and new applications support and the applications' having very specific and differing characteristics results in calls and sessions which will traverse multiple network elements and facilities and will switch between different paths for signalling or bearer functions. Thus, many more reference connections will be needed for reliability design.

3.1.2.2. Additional Failure Sources in Reliability Design

Current reliability designs typically ignore a large class of potential failures because they either have little impact on reliability or did not exist for the PSTN. For example, while central office power is critical to network reliability, its robustness contributes very little to overall network reliability. However, future networks will have more elements that are AC-powered and, hence, susceptible to increased power fluctuations and power transients compared to DC-powered equipment. Critical elements may also be placed in non-Central Office environments, putting them at increased power failure and security risk. Thus, power reliability should be included in the network reliability design.

Network operators and service providers are always concerned about the reliability involved with introducing new equipment and software into the network. This is an even greater concern for the future networks because of the total number of new elements and the amount of software, the number of vendors within a network and the related interoperability issues. There will be a need for reflecting the reliability of this new environment (e.g., software patch installation, maturity curve of hardware and software, interoperability).

3.1.2.3. Increased Number of Network Layers

The future networks will have added layers (e.g., Ethernet, MPLS), on top of access networks to implement the new services. For example, IMS is a layer above these. The current approach often represents the underlying layers by a "cloud" with generic availability (e.g., often 100% availability). This may suffice for legacy networks, however, such assumptions for the many layers of the future networks, may be overly optimistic.

3.1.2.4. Future Networks Introduce More Variability

Designers typically work with averages and ignore the parameter and system variation. This may be safe for legacy networks with limited applications, fewer call paths, and whose equipment has less reliability variation due a long history of field operations. However, in future networks, the number of applications and the paths they take is large. Due to the flexibility of functional implementation, call paths could also vary depending on the implementation. A user could experience dramatically different reliability (and security) based on where and how the functions are implemented. Therefore, taking into account the variability and statistics is more important for the future networks. An additional benefit will be better formulation of SLAs with the end-customer and with the vendors.

3.1.2.5. Significant Point of Failure

Significant Point of Failure (SgPOF) is a new concept superseding Single Point of Failure (SPOF) for future networks. The numerous applications and network functions of future networks rely heavily on disaggregated customer and network databases, applications servers and session states. Total failure may not occur, but a significant number of subscribers may experience an outage or serious performance degradation. Thus, it becomes more important to include a SgPOF step in the network design which looks at the impact of element failure on the service. It measures the impact in terms of the likelihood of failure, loss of bandwidth and connectivity, and the affected number of service subscribers. It prioritises those failures for redesign.

3.2. Network Operations

Network operations plays a key role in network reliability. Decades of root cause analyses for network outages point to a very high number of outages caused by operations related events. In this section we highlight reliable network operations and procedural reliability.

3.2.1. Reliable Network Operations

Although it is recognised that reliable network operations is essential for preventing outages, outages due to operations factors still occur. For example, more than half of the Application Service Provider (ASP) executives asked to report on the incidence of unscheduled downtime (i.e. outages) within their organisation, experienced unscheduled downtime in the last 12 months[60]. The increasing number and complexity of applications in the future networks will likely increase incidences unless specific care is taken in the following areas.

3.2.1.1. Skilled Personnel and Field Experience

New entrants could be quick to enter the market and traditional providers in trying to quickly introduce new technology may not have an adequate number of highly experienced, skilled or trained workers. Provisioning, deployment, operation, and maintenance skills for legacy networks are available and can be useful in the transformation to the future networks. However, experience in deploying and scaling the future networks has not yet developed. In general, the transformation steps, the data preservation and population for the future networks is beginning to be worked out. The understanding on how the databases, servers, and capacity will scale will come as loads increase on the new networks.

3.2.1.2. Challenges Due to Increased Complexity

Network operators are assuming that moving to the future networks will reduce overall operating costs that they can transform the network infrastructures without interrupting current service, and they can maintain high levels of customer satisfaction through speedy and flawless service delivery. The complexity of the future networks, however, presents challenges to reliable network operations that affect network reliability and security. Examples include:

- Multiple technologies and significant numbers of vendors within the same network
- Europe's high degree of inter-network connections
- Convergence of multiple services and applications on the same network
- Multi-Service Provider (Application Service Providers, content providers, network operators, enterprises) environment
- Multi-location (regions) interfaces and interactions

60 IDC's Survey of ASP Infrastructure Systems Software, 2000

- Multi-media, multi-services management as an integral part of network operations
- End-to-end service security, availability, QoS and SLAs

Although some of these are found in legacy networks, they will be much more pronounced in the future networks.

3.2.1.3. Software Upgrades

Software companies develop new versions to maintain a competitive edge and point releases and patches to address problems and to stay ahead of the viruses, worms and other attacks. There is a trade off between placing this software in service and doing thorough regression testing with the other software in the network. Thus, the viruses, worms, and other attacks, plus the potentially inadequate regression testing make the future networks potentially more prone to decreased reliability.

3.2.1.4. Interoperability Testing

Rigorous interoperability testing prior to cutover of software and hardware has been the norm for the incumbent services providers and one way in which they achieved high reliability. Service introduction and software and hardware upgrades were carefully timed. The future networks have much more multi-vendor software and hardware to enable their multi-services capabilities. More attention to interoperability and regression testing is needed to integrate the multiple vendors' products as well as to integrate two or more technologies and multiple network gateways and connections. The testing is also dependent on the thoroughness of supplier testing. Thus, due to this increased complex environment and the varying level of testing resources in all these entities make the future networks more prone to decreased reliability.

3.2.2. Procedural Reliability

Procedural reliability refers to reliability issues related to the human aspect of the network, including the operating personnel, documentation and training. Surveys have indicated that the lack of procedural reliability is a major, if not the highest, source of network failures. And that human error is a significant factor in reliability for a number of other industries (e.g., power, aviation, manufacturing, and transportation).

Education lags the rapid growth of new technologies and without operator personnel's awareness of reliability and security issues, they are likely to precipitate these procedural errors.

The complex multi-vendor, multi-technology future networks also increase the chance of human error. New methods and procedures, and Operations Support Systems (OSS) and Business Support Systems (BSS) are needed for the more distributed functions. These increase the chance of human error when manual intervention is needed[61],[62]. Procedural outages account for 45% of the cable electronics attributed facility outages. They are a major (52% frequency) root cause of local switch outages. They are the dominant (46%) cause of Common Channel Signalling (CCS) outages, and they account for 52% of Central Office power outages.

61 Network Reliability Steering Committee (NRSC), "Network Reliability Steering Committee Annual Report, 2001" www.atis.org/NRSC/Docs/2001rpt.pdf .

62 ATIS, "Procedural Outage Reduction; Addressing the Human Part," NRSC Report May 13, 1999.

Disaster recovery and emergency preparedness policies, plans and management will need to be reworked because of the new networks, services, equipment, operating environments and technologies. There is a wide range of stakeholder starting points and experience. New entrants will have to develop these plans from the beginning. Until the new practices are ingrained, informal and ad hoc responses to emergencies may occur.

The increase in Internet commerce providers and new entrants has also lead to more sharing of office space and resources with other service providers and the use of leased space arrangements and the risk of other operators negatively impacting adjacent operations. Personnel at these locations will need to understand their responsibilities, what support and resources they will get from other providers at the location and how the site business continuity, disaster recovery, and security plans fit into their own company plans. Without this understanding and adequate training, they may compromise shared resource and create procedural errors for others, which could lead to failures for all.

3.3. Network Resource Management

In the transition to future networks from the PSTN/IN, subscribers generally received adequate performance even though the providers offered only “best effort” services. This was true since there was excess capacity throughout the network for the services the subscriber was accessing and the services being offered were relatively simple and had few quality of service (QoS) requirements (e.g., Instant Messaging, e-mail). The future networks will offer VoIP, IPTV, broadcast Internet radio, video conferencing and many related services such as video telephony and gaming. The bandwidth and QoS demands on the network are therefore increasing and for the first time it is likely that the network capacity will be more fully used and that there will be a true need to differentiate multiple services on the same network. Moreover, signalling and operations traffic are not physically separated from bearer traffic on the future networks and may be more subject to congestion due to bearer traffic overload. The challenge will be to provide end-to-end QoS required across all services and network functions.

An admission control function[63], including policies and network resources, will be needed to address the new bandwidth and QoS requirements. This will avoid service degradation to the point of unavailability. The function can be provided directly by the network or service providers or via the application, services or content providers.

Without adequate admission controls, calls, connections or sessions could be established that exceed overall engineered network capacity, resulting in lost packets and lower QoS for all subscribers. More operators are making decisions on admission control requirements, where in the past they have relied on over engineering. Others believe they can more cost effectively provide excess capacity.

There is a risk in running the network/service without explicit controls, however. Even with excess capacity, there will always be focused overload conditions (e.g., caused by special advertising events, contests and emergencies). Thus, just when QoS is needed, it will not be achieved due to the lack of controls . In addition, the expected growth in Europe’s traffic from the new services will erode the excess capacity.

63 ITU-T RACF and ETSI/TISPAN RACS address functional elements which address access control. RACS is more focused on access and preceded RACF which is more focused on the core network. There is an effort to harmonise the two.

3.4. Impact of Security Vulnerabilities

The connection between security and availability should not be overlooked. The future networks and IP-based services will be subject to many types of threats attempting to exploit the vulnerabilities inherent in IP networks and the increased dependence on software for the new applications. Mission critical applications and the network infrastructure are at risk. For example, Denial-of-service (DoS) attacks, such as Code Red and NIMDA cause service and application disruptions[64].

X.805 and other analyses identified threats and vulnerabilities, if successfully exploited, that would affect the future network availability. Some of the threats "leak" back to and expose vulnerabilities in the legacy networks, such as the PSTN/IN, because of the gateways between the future and legacy networks.

3.4.1. Security Attacks

Availability is one of the eight security dimensions in the X.800 and X.805 model and framework. Consider the 3GPP/3GPP2 IMS architecture as an example of linking security and availability. The S-, P- and I-CSCFs, in particular, are customer, network and external network facing devices that are vulnerable to DoS attacks. Even with hardware and software fault tolerant implementations (e.g., implemented as redundant and failover systems), a security vulnerability, if present, will appear in both the active and standby system. Thus, a DoS attack could bring down both the active and the standby systems. There is a need to decide on how to treat the effects of security breaches to minimise service downtime.

3.5. High Degree of Interconnection

A high degree of network interconnectivity is characteristic of the European future network environment. A common, appropriate level of network availability and robustness is required because subscribers are likely to use applications and services which span multiple networks. Networks which are weak links, (e.g., lower the overall reliability and security of the interconnected European communications infrastructure) will need to be improved. This may be a challenge, given the economic capabilities of new entrants versus incumbents, and newer versus older EU Member States and their differences in national economies.

3.6. ISP Network Design Affects More than the ISP Network

The Internet ISP network design should consider how it may inhibit cascading failures, as well as how to achieve its own reliability[65]. Common ISP network designs may trade off reliability. For example, ISPs use hub-and-spoke networks for connections to peer and exchange traffic at strategic locations. These have distinct economic advantages over mesh networks since they consolidate flows across a few high-bandwidth connections. However, these are relatively unprotected against, and vulnerable to, cascading failures[66].

64 J.T. McKelvey, "Combatting Security Risks on the Cable IP Network," IBC 2002 Conference, http://www.broadcastpapers.com/ibc2002/ibc2002.html.

65 T.H. Grubesic, M.E. O'Kelly, and A.T. Murray 2003. A geographic perspective on commercial Internet survivability, Telematics and Informatics 20: 51-69.

66 T. H. Grubesic and A. T. Murray: "Vital Nodes, Interconnected Infrastructures, and the Geographies of Network Survivability, Annals of the Association of American Geographers, 2006.

3.7. Congestion

Congestion (i.e. network congestion and degraded latency and throughput performance) make the loss of a node significant for a geographically linked network. When a failure causes traffic to be switched to alternate paths on the same network or to be transferred to other networks, the routers may be unable to find adequate capacity on an alternative path, latency can increase, and cascading failures may arise.

3.8. Asset Concentration at Vital Nodes

Network Access Points (NAPs) and Internet Exchange facilities are pivotal interconnection and collocation points for the commercial Internet, providing affiliated networks with peering and data transit options. Hundreds, possibly thousands, of similar, smaller-scale interconnection points are located in Europe. Concentration in single locations has the potential for a series of targeted attacks to do significant damage to the functionality of the commercial Internet. The loss of a local network can not only isolate local subscribers, but also significantly decrease the overall bandwidth available to the Internet.

3.9. IP Network Reliability

3.9.1. IP-Networks and Equipment Have a Choice of Reliability Features

Fault tolerant routers and switches provide redundancy within and between the equipment using fast, high availability procedures for failovers. The networks can also support redundant links as well as access redundancy. Network reliability can be enhanced with deployment of fault-tolerant, redundant network elements and implementation of high availability features, load sharing/hot-standby links and access redundancy. Figure 35 shows a few logical networking functions that help maintain redundant paths and provide failover.

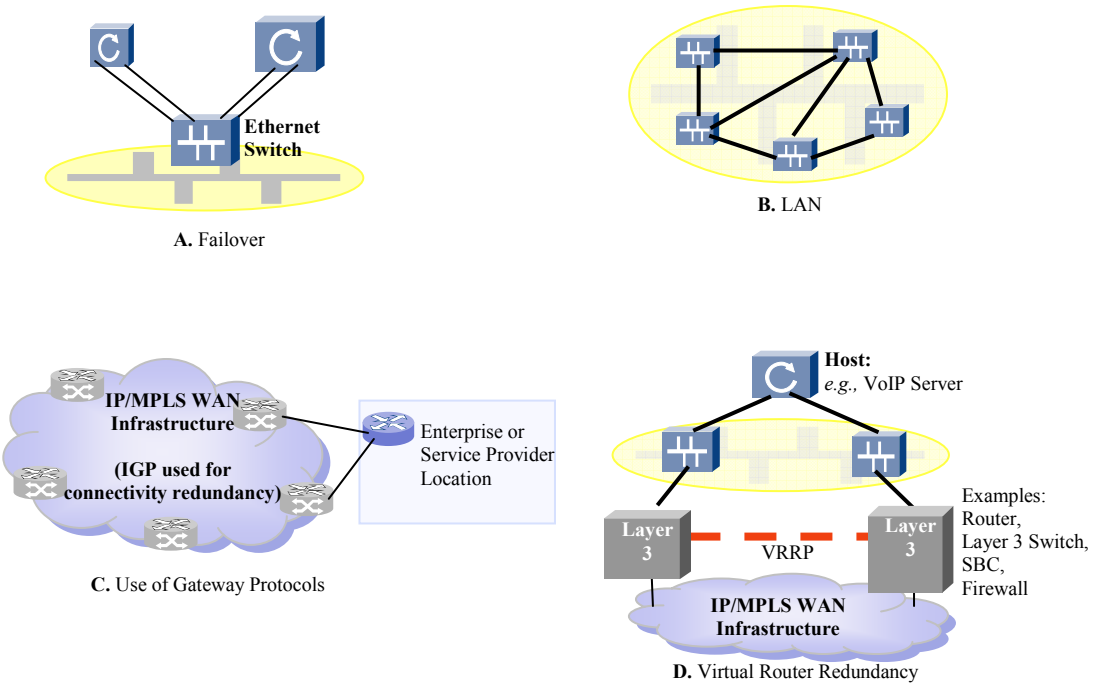


Figure 35: An Example of Implementing Network Reliability in a VoIP Network

Some server products may provide proprietary fail-over (Figure 35A) capability (e.g., SUN® Solaris multi-path technology) between its Ethernet ports connecting to the Ethernet switch of the LAN.

In the Ethernet LAN, redundancy (Figure 35B) of connectivity between two switches is provided by use of spanning tree or rapid spanning tree protocol. Link aggregation may also be used.

Assuming that any two routers can have at least two physical paths between them, the network Interior Gateway Protocol (IGP) such as OSPF or IS-IS will dynamically determine the best available path. Service provider locations and strategic enterprise locations may connect their routers to two different routers for access redundancy. Protocols such as BGP will maintain access connectivity over one of the two links (see Figure 35C).

VRRP or Virtual Router Redundancy Protocol (Figure 35D) provides accessibility to the host even if the connectivity to the WAN through one of the Layer 3 device (say, router) is lost.

3.9.2. Options for Powering IP Phones

There are a variety of methods for powering IP phones, each of which has a different impact on reliability. For example, IP phones and gateways, connecting the analogue phones could use battery back-up or UPS in case of power failures. Enterprise IP phones are connected to the LAN and Power over Ethernet (PoE) technology could be used. However, UPS is needed to power the LAN/PoE itself. The impact should be understood, before making the selection of this technology.

3.9.3. Emergency Calling

Implementation of emergency calling on future networks is not yet clearly or uniformly laid out. Service providers, that handle public-to-authority emergency calls, face the unresolved VoIP nomad problem. A common work around puts the burden on the subscriber to update their information on a website each time they move their IP phone to different physical location.

Authority-to-public calls (i.e. the ability of an authorised agency to place a warning call to all subscribers in an area) are not supported, even in the cable networks. ITU-T SG 2 has created authority to public requirements. In the U.S. there is activity in the FCC to quickly create the service as required by the Warning, Alert and Response Network (WARN) act enacted on 13 October, 2006. Standards work is underway to provide procedures and protocols that support international emergency calling. Member States may need to establish national policies and international agreements to support these calls.