1/19/2017

# Report on Implementation of Evolving Telecommunication/ICT Infrastructure for Developing Countries

Report on Implementation of Evolving Telecommunication/ICT Infrastructure for Developing Countries

(Input Document to ITU-D Q.1/1 and Q2/1)

December 2016

# Table of Contents

## 1. Introduction

This input document to ITU-D Study Group 1 aims at presenting a comprehensive view of technical, economic and policy aspects in support of network key convergences. It contemplates relevant international ITU standards for each topic covered.

Contributed to this report Study Group Rapporteurs and collaborators, as well as ITU staff from all three sectors.

## 2. Objectives

The Report covers aspects related to the deployment of telecommunication/ICT networks, including rural applications as well as core, access and home networks. Network operation and management are also considered. The Report further identifies key issues for broadband networks such as universal access, emergency services and environmental aspects while offering various convergence issues that are relevant to developing countries.

The ultimate objective of this input is to provide insightful information to assist ITU-D Study Groups participants in advancing the work of the Question and ultimately in helping Membership establish their national strategies towards a telecommunication/ICT infrastructure for the benefit of telecom industry, their consumers and businesses.

## 3. Telecommunication/ICT Infrastructure: technology, economic and policy aspects

"Robust telecommunication/ICT infrastructure is considered to be an underpinning and enabling platform that should be universally available and accessible to all people to enhance a global economy and information society, and high-speed communication networks directly promote innovation throughout economies as much as electricity and transport networks, among others"

*Dubai Declaration – World Telecommunication Development Conference 2014*

### 3.1 Mobile Broadband Access Networks

Mobile broadband is a mainstay of information and data communication. The last decade has seen an explosive growth in mobile telephony in all countries. Rapidly falling costs and technological progress have made connectivity to rural and remote areas feasible[1]. With the growth of mobile communications, coupled with the evolution of IMT, operators in developing countries are establishing mobile networks in unserved and/or underserved areas, upgrading their existing networks and integrating new technologies which have to coexist and interoperate with existing ones.

#### 3.1.1. International Mobile Telecommunication (IMT)

The framework of standards for International Mobile Telecommunications (IMT) encompasses IMT-2000 and IMT-Advanced which spans the third and fourth mobile generations' industry perspective.

- Overview of IMT-2000

International Mobile Telecommunication-2000 (IMT-2000)[2], third generation mobile systems started service around the year 2000, and provide access by means of one or more radio links to a wide range of telecommunications services supported by the fixed telecommunication networks (e.g. public switched telephone network-PSTN/ Integrated Services for Digital Network-ISDN/Internet protocol-IP) and to other services specific to mobile users. Since then, IMT-2000 has been continually enhanced.

IMT-2000 systems are defined by a set of interdependent Recommendations. Among them, ITU -R M.1457 forms the final part of the process of specifying the radio interfaces of IMT-2000, as defined in Recommendation ITU-R M.1225. It identifies the detailed specifications for the IMT-2000 radio interfaces.

- IMT-Advanced

After the Radiocommunication Assembly (RA-12)[3], in Geneva, 16-20 January 2012, consensus was reached to expand the IMT Radio Interface family by establishing the new IMT-Advanced standard. The Recommendation ITU-R M.2012[4] dealing with IMT was approved by all Member States.

  - Definition

    International Mobile Telecommunications-Advanced (IMT-Advanced) systems are mobile systems that include the new capabilities of IMT that go beyond those of IMT-2000. Such systems provide access to a wide range of telecommunication services including advanced mobile services, supported by mobile and fixed networks, which are increasingly packet-based.

---

[1] ITU-D webpage on Mobile Communications: http://www.itu.int/en/ITU-D/Technology/Pages/MobileCommunications.aspx

[2] ITU publications that contributed to this this section include: ITU-R M.1457 - Detailed specifications of the terrestrial radio interfaces of International Mobile Telecommunications-2000 (IMT-2000); and ITU-R Q.1740-series - Supplement on scenarios and requirements in terms of services and deployments for IMT and IMS in developing countries.

[3] IMT-Advanced webpage: http://itu.int/go/QJ9R.

[4] ITU-R M.2012: Detailed specifications of the terrestrial radio interfaces of International Mobile Telecommunications Advanced (IMT-Advanced), 2015.

IMT-Advanced systems support low to high mobility applications and a wide range of data rates in accordance with user and service demands in multiple user environments. IMT Advanced also has capabilities for high quality multimedia applications within a wide range of services and platforms, providing a significant improvement in performance and quality of service.

- Key features of "IMT-Advanced"
  - a high degree of commonality of functionality worldwide while retaining the flexibility to support a wide range of services and applications in a cost efficient manner;
  - compatibility of services within IMT and with fixed networks;
  - capability of interworking with other radio access systems;
  - high quality mobile services;
  - user equipment suitable for worldwide use;
  - user-friendly applications, services and equipment;
  - worldwide roaming capability; and,
  - enhanced peak data rates to support advanced services and applications (100 Mbit/s for high and 1 Gbit/s for low mobility were established as targets for research)[5].

These features enable IMT-Advanced to address evolving user needs and the capabilities of IMT-Advanced systems are being continuously enhanced in line with user trends and technology developments.

- Functional network architecture for IMT-Advanced

The functional architecture incorporates the following general principles[6]:

- Network based on IP technology
  - Access networks, which provide a rich set of access mechanisms using various wired and wireless access technologies, terminate layer two link characteristics and provide IP-based connection to core networks. Core networks and application servers connected to them are IP based.
- Modular construction using expandable components
  - The subsystems themselves, such as access networks, core networks, and application servers; as well as the systems built based on them are hierarchical. In particular, core networks provide universal interfaces to different access networks and to all kinds of application servers;
  - Accessibility to each subsystem is separately controlled based on each operator's policy; on the other hand in particular, paths that users can control to access application servers are prepared.
- Open interfaces between various systems
  - Interoperation with homogeneous networks and with heterogeneous networks is facilitated with open interfaces in various levels of subsystems.

The IMT-Advanced architecture should support multiple access networks, converged services in a converged network, enhanced security and protection, and total service accessibility, based on the services and network capabilities framework of network aspects defined in [ITU-T Q.1703] and aligned with the NGN architecture.

- NGN architecture overview

  The NGN architecture is based on the general principles defined in [ITU-T Y.2011]. It is further detailed in [ITU-T Y.2012] for transport and service stratum functions and in [ITU-T M.3060] for management functions that apply to both transport and service strata.

---

[5] Data rates sourced from ITU-R M.1645 - ´Framework and overall objectives of the future development of IMT-2000 and systems beyond IMT-2000´.

[6] ITU-T Q.1704: Functional network architecture for IMT-Advanced (2008).

- IMT-Advanced architecture overview and NGN

  The IMT-Advanced architecture is based on the general principles defined in [ITU-T Y.2011]. It is not necessarily identical to the NGN architecture because of additional functions derived as a consequence of addressing mobility, recognizing that these two architectures are moving towards convergence.

### 3.1.2. Satellite Component of IMT

The terrestrial and satellite components of IMT are complementary, with the terrestrial component providing coverage over areas of land mass with population density considered to be large enough for economic provision of terrestrially-based systems, and the satellite component providing service elsewhere by a virtually global coverage. The ubiquitous coverage of IMT can only therefore be realized using a combination of satellite and terrestrial radio interfaces[7].

- Satellite Component of IMT-2000[8]

IMT-2000 is defined by a set of interdependent Recommendations. Recommendation ITU-R M.1850 forms the final part of the process of specifying the radio interfaces of IMT-2000, as defined in Recommendation ITU-R M.1225. It identifies the detailed specifications for the IMT-2000 satellite radio interfaces.

Updates and enhancements to the satellite radio interfaces incorporated in Recommendation ITU-R M.1850 have undergone a defined process of development and review to ensure consistency with the original goals and objectives established for IMT-2000 while acknowledging the obligation to accommodate the changing requirements of the global marketplace. Figure 3-1-1 shows the various interfaces in the IMT-2000 satellite component.

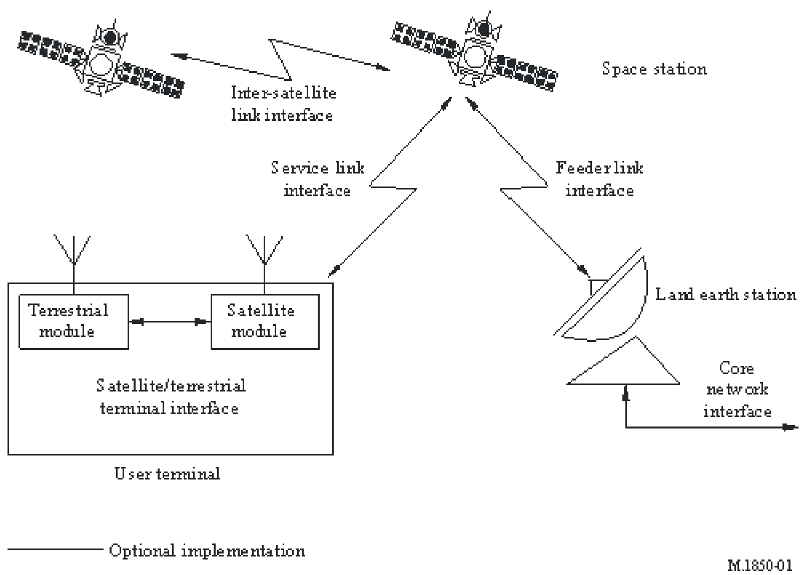



Figure 3-1-1. Interfaces in the satellite component of IMT-2000

[7] For more information on Global Circulation of IMTsatellite terminals, see Recommendation ITU-R M.2014-1 (2015).

[8] Recommendation ITU-R M.1850-2: Detailed specifications of the radio interfaces for the satellite component of International Mobile Telecommunications-2000 (2014).

- **Satellite component of IMT-Advanced**

As the terrestrial component alone would not be deployed all over the world, the satellite component of IMT-Advanced systems would be complementary in order to provide a seamless service with global coverage[9].

As mentioned above, the integration between satellite and terrestrial components of IMT-Advanced is required in order to effectively utilize the respective areas of strength of each network within their traditional roles and mandate. An integrated satellite and terrestrial network can contribute to the emergence and utility of Next-Generation Networks (NGNs) in providing ubiquitous and universal broadband versatile IP-based services to end users who will require generalized mobility, accessed in a seamless fashion and, ultimately, will dictate its realization through market forces. A typical large-scale integrated system comprises multi-beam satellites and a nationwide or regional ensemble of Complementary Ground Component (CGC) and terrestrial components wherein both satellite and CGC segments communicate with user equipment using a common set of mobile-satellite service (MSS) frequencies to handle broadcasting scenarios, while terrestrial components use a separate set of frequencies to provide ubiquitous coverage of broadband two-way communications to end users with generalized mobility requirements.

***System Aspects[10]***

The satellite component of IMT-Advanced is expected to have sufficient power and receiver sensitivity to establish communications with end-user devices that are indistinguishable from the terrestrial component. Large satellite antennas, providing high-gain reconfigurable multi-beam are one of the key attributes of integrated systems. These features enable increased spectrum reuse as well as communications via typical low-cost handheld terminals. User equipment of an integrated system should have the capability of selecting the relevant component – either the satellite- or terrestrial-based – on the receiving signal level and network availability to keep a given service quality over a wide and continuous service area. It would be preferable that the integrated system could have roaming capability with a unique user/subscriber identifier across both terrestrial and satellite components. Handover between satellite and terrestrial components in an integrated system should be carried out within the extent that execution of handover does not significantly decrease the system capacity or increase system complexity.

A concept for this integrated system is shown in Figure 3-1-2.

---

[9] For more information on the Satellite Component of IMT-Advance see:

- Recommendation ITU-R M.2047 - Detailed specifications of the satellite radio interfaces of International Mobile Telecommunications-Advanced (2013)
- Reeport ITU-R M.2279 - Outcome of the evaluation, consensus building and decision of the IMT-Advanced satellite process (Steps 4 to 7), including characteristics of IMT-Advanced satellite radio interfaces (2013)

[10] Report ITU-R M.2176-1 - Vision and requirements for the satellite radio interface(s) of IMT-Advanced (2012)

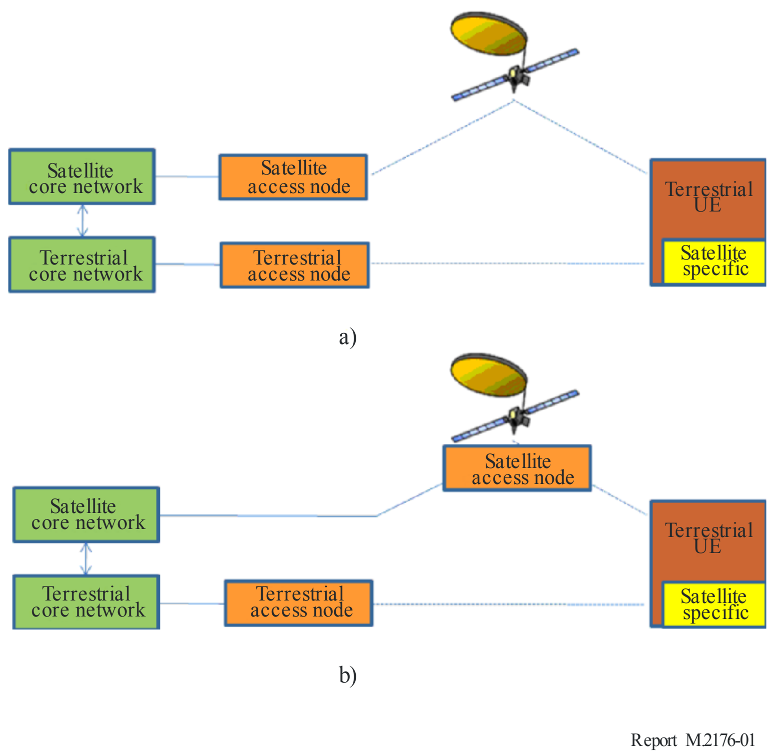



Fig. 3-1-2 Possible system architectures for the satellite component of IMT-Advanced

### *Possible system architectures for the satellite component of IMT-Advanced*

Figure 3-1-3 describes an overall system architecture presented by Report ITU-R M.2176 for the satellite component of IMT-Advanced. The following factors can be considered:

– Satellite component: It will provide services and applications similar to those of the terrestrial component beyond terrestrial and CGC coverage, under the inherent constraints imposed by power limitation and long round-trip delay.

– CGCs: In order to provide mobile satellite broadcasting/multicasting services, they can be deployed in areas where satellite reception is difficult, especially in urban areas. They may be co-located with terrestrial cell sites or standalone. Several kinds of CGC can be considered, such as simple amplifying and forwarding CGC acting as simple repeaters, a demodulation and forwarding CGC for high modulation and a decoding and forwarding CGC for better traffic quality. It would require careful consideration to use the same frequency band in the satellite component and CGC, since the CGC would possibly cause harmful interference to their own terminal or radiocommunication systems which are operated in the adjacent band and which do not expect that the adjacent band originally allocated to the satellite component is used also for the CGC with higher power density than the satellite's one.

– Terrestrial component: The satellite component can provide voice and data communication services in regions beyond terrestrial coverage. The areas not adequately covered by the terrestrial component include physically isolated regions, gaps in the terrestrial network coverage and areas where the terrestrial infrastructure is permanently, or temporarily, destroyed in the event of a disaster. In order to provide the terrestrial fill-in service, vertical handover of the satellite component with terrestrial component is considered one of the most important techniques.

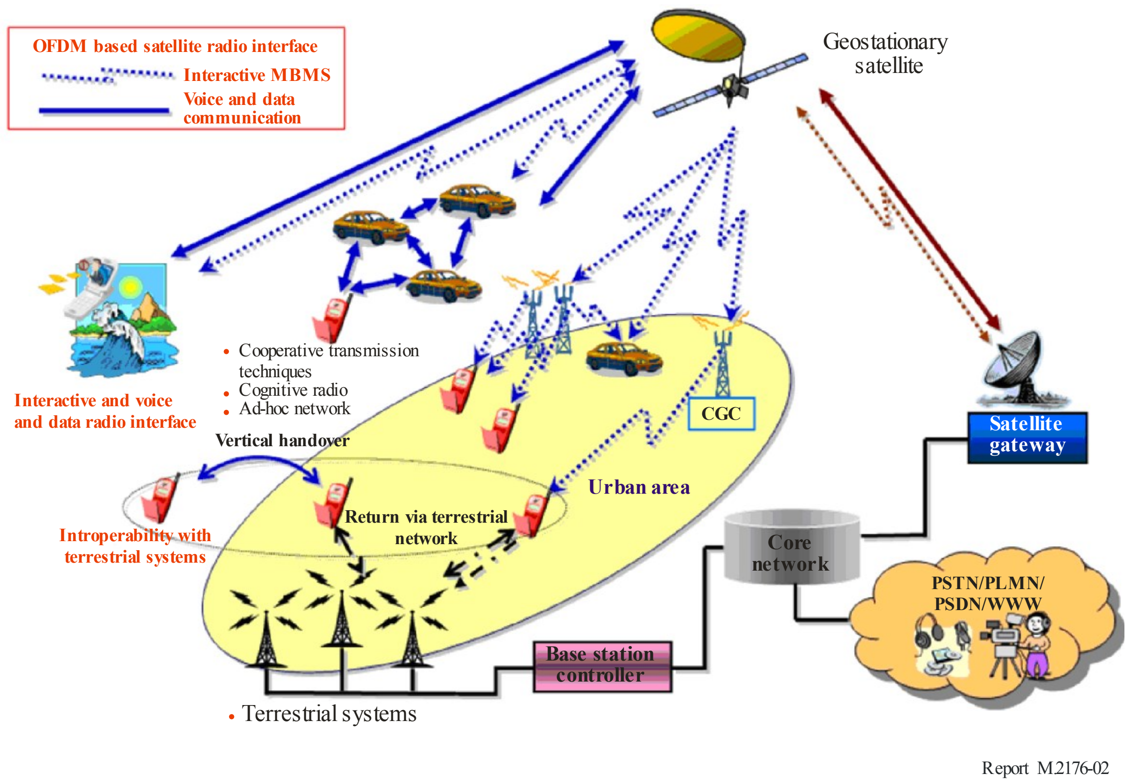



Figure 3-1-3 - Overall system architecture for the satellite component of IMT-Advanced

### 3.1.3. IMT for 2020 and beyond

In early 2012, ITU-R embarked on a programme to develop "IMT for 2020 and beyond" [11], setting the stage for "5G" research activities that are emerging around the world.

Through the leading role of Working Party 5D, ITU's Radiocommunication Sector (ITU-R) is finalizing its view of a timeline towards "IMT-2020". The detailed investigation of the key elements of "5G" are underway.

In 2015, ITU-R finalized its "Vision" of the "5G" mobile broadband connected society. This view of the horizon for the future of mobile technology in support of the growth of IMT is described in Recommendation ITU-R M.2083.

- **ITU-R Working Party 5D deliverables towards "IMT for 2020 and beyond"**

Vision and Technology Trends:

[11] ITU-R webpage: http://www.itu.int/en/ITU-R/study-groups/rsg5/rwp5d/imt-2020/Pages/default.aspx

- Report ITU-R M.2320: This activity is to address the terrestrial IMT technology aspects and enablers considering the approximate timeframe 2015-2020 and beyond for system deployment, including aspects of terrestrial IMT systems related to WRC-15 studies as part of its scope.
- Recommendation ITU-R M.2083: This activity is to address the longer term vision for 2020 and beyond and will provide a framework and overall objectives of the future developments of IMT.
- Report ITU-R M.2376: The purpose of this report is to provide information on the study of technical feasibility of IMT in the bands above 6 GHz.

Additional reference to the progress of studies on IMT-2020 and all documentation relating to IMT can be found on the ITU-R Working Party 5D website: http://www.itu.int/en/ITU-R/study-groups/rsg5/rwp5d/Pages/default.aspx

- **ITU-T Study Group 13 decisions on IMT 2020 and beyond**

  During the SG 13 meeting held in April 2015, ITU has established a new Focus Group to identify the network standardization requirements for the '5G' development of International Mobile Telecommunications (IMT) for 2020 and beyond. The Focus Group's scope of activity is concentrated in identifying the standardization needs of the wireline elements of 5G networks, building on an analysis of other entities' IMT-2020 studies. ITU-T standardization activity based on the findings of the Focus Group will prioritize the alignment of its IMT-2020 deliverables with those of ITU-R, ensuring that standardization work on the network aspects of IMT-2020 supports the further evolution of IMT.[12]

### 3.1.4. Consideration for developing countries[13]

- **Expected Benefits from IMT for Developing countries**

While IMT offers many benefits, developing countries need to rationalize their expectations for implementing the technologies. When deciding and justifying the implementation of IMT, developing countries need to carefully analyse, understand, balance and prioritize the benefit in order to get the best from the implementation.

Each developing country has its unique expectations on the benefits and these should play a key role on the decision as to whether to implement IMT. For example, while most developed countries are keen on achieving high bit rates, quality of service and better utilization of scarce resources, the priority of most developing countries is in taking affordable services to their rural and underserved areas.

Generally, the most common expected benefits that most developing countries have from IMT as new technologies include:

- Addressing convergence between mobile and fixed services;
- Backward compatibility with existing networks;
- Bring the country up to date with current technology (modernization);
- Efficient utilization of electricity;
- Meeting the need for affordable  and economical solutions for rural communication needs;
- Billing accuracy;
- Quality of Experience (QoE);
- QoS;
- Security;
- Spectrum efficiency for wireless technologies;
- Support of modern services (data and multimedia) while maintaining voice services; and
- Increasing revenue streams from mobile operations.

[12] The Focus Group IMT-2020 plans to conclude its study till December 2015. For more information see http://itu.int/go/B08Y.

[13] This section is based on the ITU-T Supplement Q.1740-Series – *Supplement on scenarios and requirements in terms of services and deployments for IMT and IMS in developing countries*, developed under ITU-T SG 13.

Developing countries should therefore carefully look at IMT to see how well they respond to their unique requirements including the above benefits before they can wholly embrace implement. Each developing country is encouraged to strike a balance on its priority taking into account its unique national aspirations.

The following shows more specific benefits from implementation of IMT.

- Capabilities and Services

  IMT access technologies (e.g. LTE) provide higher bandwidth for mobile networks for launching newer services. These technologies further support effective spectrum utilisation resulting in cost effectiveness.

  Developing countries should thus be desirous to improve and modernise their telecommunication infrastructures which are largely based on telephone oriented service, such as, PSTN/ISDN.

- Operational

  Key features of IMT are contained in Recommendations ITU-R M.1645, ITU-R M.1822, and IMT-Adv/2 Rev.1[14] and include:

  – Less capital intensive compared to fixed networks;
  – Easier to manage ;
  – Improved reliability;
  – Technical and interoperability requirements available for integration testing;
  – A lot of commonly available support (similar systems);
  – higher degree of commonalities in a global scale;
  – compatibility of services within former IMT-2000 networks and fixed networks;
  – higher quality;
  – smaller terminals for worldwide use;
  – worldwide roaming capability;
  – capability for multimedia applications, and a wide range of services and terminals;
  – Better Average Revenue Per User (ARPU).

- Catching up with modern trends (Technological and otherwise)

  In developing countries, the task of bridging the digital divide arrived at a juncture where most of these countries were still grappling with the problem of providing voice access. Large-scale computerization and growth of e-services require availability of higher bandwidth on the local access network. In these countries, most of the access networks are likely to be implemented using wireless technology and, therefore, IMT systems have a unique advantage in these markets.

- Resource management

  Developing countries have the responsibility of managing resources well. These days, developing countries are very concerned about whether new technologies, innovations and systems utilize resources efficiently.

- Electricity Requirements

  Likewise, developing countries have a genuine concern for systems and their requirement for electricity. In many developing countries, electricity is expensive and only available in cities and major towns, leaving most of the rural places without commercial electricity. These rural areas can only be serviced using alternative sources of power such as solar and wind power electricity. Consumption is a key factor in deciding the type of communications systems to adopt.

- Health and Environment

  Countries are becoming more cautious about ICT technologies and their effect on health. Developing countries are keen to be satisfied that new systems and technologies do not pose environmental and health risks.

[14] This document describes the process and activities identified for the development of the IMT-Advanced terrestrial components radio interface Recommendations, and can be found at http://itu.int/go/P1GH.

- Consumer Issues

  On behalf of the consumer, governments in developing countries are usually concerned about:

  – End user terminal availability, including cost;
  – Availability of end user terminals in conformance with international standards and/or regional technical requirements, such as spectrum allocation;
  – Technical assistance, seller's guarantees and after sales services;
  – Interoperability capabilities between different vendors and legacy networks;
  – Service cost;
  – QoS;
  – QoE;
  – Availability;
  – Suitability for rural utilization;
  – Environmental and Health;
  – Ease to use.

  For any new system or technology to be considered favourably, it should be able to address the above listed issues.

  Globally, there is documented evidence that IMT operators are experiencing increasing growth in ARPU and most of it can be directly attributed to users adopting and using packet data services.

- **Implementation of IMT in mobile networks of developing countries**

Generally, implementation of IMT requires the availability and access to the IMT spectrum. This is a big challenge in some developing countries because they may not have anticipated these requirements and may have already assigned the resources needed. And now there are hardly reasonable quantities of spectrum in the required IMT bands. A number of developing countries have been able to overcome this by issuing 3G licenses in the higher bands which had not been allocated to other uses. Therefore, spectrum re-planning and reforming might be necessary in some countries.

Due to the high cost of implementing IMT, some developing countries are considering a shared infrastructure approach to reduce the cost burden on individual operators[15].

In developing countries, the rate on implementation of these new technologies and systems is still low. In a number of developing countries, some operators have just invested in legacy networks and are reluctant to invest in new technologies before they recoup their investment. Furthermore, where governments in developing countries are part owners of networks, it is important to justify to them the need to spend additional money for newer technologies.

Reasons for the slow implementation differ from country to country but generally they relate to:

- Insufficient information on the benefits of the new technologies and systems;
- Lack of conformance and interoperability;
- Lack of required capital;
- Not being able to pursue network owners to implement;
- Lack of infrastructure;
- Expensive spectrum;
- Unavailability of required spectrum;
- Inadequate policies.

ITU and other Standards Development Organizations (SDO) have published technical papers on the implementation of IMT from commonly existing networks and provided reasons, justification and recommendation for each implementation path. However the general issues that are of particular importance for developing countries include:

[15] A detailed description of IMT technical implementation can be found in the ITU Handbook on Migration to IMT-2000 Systems, available at: http://itu.int/go/1X8P.

- The state of existing networks and migration to NGN/IMT networks[16];
- Availability of IMT spectrum; and
- Capital.

Most of the technical considerations that are valid for developed countries are valid for developing countries. However the difference is that most developing countries have legacy networks in which they have invested a lot of money which they do not want to write-off.

A major incentive for investors to implement IMT is availability of spectrum. With the availability of IMT spectrum at reasonable costs, experience in many developing countries is that there are many investors willing to establish networks. When engaging such investors, developing countries should make it a condition that the network being built must be capable of supporting the latest IMT capabilities.

Other important requirements to investors include:

- Requirements expansion of the systems to underserved areas;
- Availability of funds;
- Affordability;
- Quality of Service (QoS);
- Quality of Experience (QoE).

Whereas developing countries may not need to specifically place a lot of attention on the above issues while implementing IMT, it is critical for developing countries to consider it may be beneficial for them to think of IT networks as solution for rural expansion, national coverage, affordability and improving QoS and QoE.

While it is not good practice to specify which technology an investor should deploy, developing countries can require specifications which favor technologies similar to those provided via IMT.

Since implementing IMT necessarily means acquisition of the requisite spectrum, developing countries should use it to leverage coverage, rural expansion, affordable services and improved QoS and QoE.

These are the global recommendations on implementing IMT:

- Technical

  The technologies are mature and stable for IMT, therefore, implementation of IMT and IMS technically present minimal risks.

  Spectrum availability and affordability is always an issue but within government control. A balance between the urgent implementation of IMT versus the price the spectrum will fetch should be well struck to enable IMT implementation.

- Economical

  IMT targets economic sense. IMT networks are more cost effective for implementation and they offer considerably better QoS and QoE while opening up opportunities for new services and higher speeds. They also offer a better choice for establishing networks in rural places.

- User experiences from other countries

  To date, there are countries that have successfully implemented IMT. There is therefore a rich user experience which can be studied.

  Many developing countries are making good use of infrastructure sharing in leveraging faster and more economical project implementation. There are countries which have considered using infrastructure sharing for implementation of some of these beneficial but capital intensive technologies and system like the IMT.

[16] ITU-D Study Groups have published a report on migration from existing networks to next-generation networks for developing countries: technical, regulatory and policy aspects, available at http://itu.int/go/KPQN.

### 3.1.5. Transition to IMT

ITU, over the last two decades, has developed a number of ITU Recommendations and Reports on IMT which could be used as reference for developing countries.

In particular, Working Party 5D has recently published (May 2015) an ITU Handbook titled "Global trends in IMT" that summarizes the work carried out and the progress towards IMT-2020. This handbook identifies IMT and provides the general information such as service requirements, application trends, system characteristics, and substantive information on spectrum, regulatory issues, guidelines for the evolution and migration, and core network evolution on IMT.

Other useful ITU publications addressing the transition to IMT and related technical papers and handbooks are listed in the table below:

| Title | Abstract | Source | year |
|---|---|---|---|
| Guidelines on the smooth transition (GST) of existing mobile networks to IMT-2000 for developing countries | These Guidelines for the Smooth Transition (GST) from the Existing Mobile Networks to IMT-2000 have been conceived to provide essential information for those who are concerned with this transition. The reader will find three threads running through the Guidelines: 1) development of policies for the transition of existing networks to IMT-2000, 2) possible transition paths, and 3) economic aspects of the transition to IMT 2000. They also provide references to related literature and ITU Recommendations | Q 18/2 | 2006 |
| Mid-Term Guidelines (MTG) on the smooth transition of existing mobile networks to IMT 2000 for developing countries; | These Guidelines are intended for use of telecom operators, policy-makers and regulators to facilitate development of their respective strategies for the transition from pre-IMT-2000 networks to IMT-2000 | Q 18/2 | 2002 |
| Implementation aspects of IMT 2000 and information-sharing on systems beyond IMT 2000 for developing countries: Supplement to GST | Supplement from ITU-D Study Group 2 Question 18-1 to the Guidelines on the Smooth Transition of existing mobile networks to IMT-2000 (GST) for developing countries. | Q 18-1/2 | 2010 |
| Multiple radio access technologies | This handbook presents the ITU-T Recommendations on next generation networks in the context of the ongoing convergence of the telecommunications and media industries | ITU-T SG 13 | 2012 |
| Migration from existing networks to next-generation networks for developing countries: technical, regulatory and policy aspects | Final Report from ITU-D Study Group 2 Question 6 on migration from existing networks to next-generation networks for developing countries: technical, regulatory and policy aspects | Q26/2 | 2014 |
| Applications of Wireless Sensor Networks in Next Generation Networks | The major goal of this technical paper is to give recent advances and state-of art results covering both fundamental principles and use cases of Wireless Sensor Network (WSNs) in NGNs. This technical paper presents design techniques and guidelines, overview of existing and emerging standards for the subject area, modelling principles for WSNs | ITU-T SG 13 | 2014 |

| | | | |
|---|---|---|---|
| How to increase QoS/QoE of IP-based platform(s) to regionally agreed standards | This Technical Paper starts with helping common understanding about key factors such as Network Performance (NP), QoS, QoE, Service Level Agreements (SLAs) and their relationships | ITU-T SG 13 | 2013 |
| Handbook on Converging networks | This handbook presents the ITU-T Recommendations on next generation networks in the context of the ongoing convergence of the telecommunications and media industries | ITU-T SG 13 | 2010 |
| Handbook on Future networks | This ITU-T handbook reviews the work to date on future networks. The development of future networks is driven by, on the one hand, the perceived challenges that are faced by networks at the moment and, on the other hand, by the continual development of new applications and technology. The work on future networks is broad in scope and covers not only technological issues but also social, economic and environmental aspects | ITU-T SG 13 | 2012 |
| Impacts of M2M communications and non-M2M mobile data applications on mobile networks | The first part of this technical paper is intended to cover both the impact of, and how to deal with, the demands of a wide variety of MTC devices. The second part of this technical paper will cover the impacts of and how to deal with "smart phones" | ITU-T SG 11 | 2012 |

## 3.2 Fixed Broadband Access Networks

### 3.2.1. Overview

- FTTX access networks

Fiber to the X (FTTX) is a generic term for any broadband network architecture using optical fiber to provide all or part of the local loop used for last mile telecommunications. The term is a generalization for several configurations of fiber deployment, ranging from Fiber to the Neighbourhood (FTTN) to Fiber to the Desktop (FTTD).

One of the most used technologies for FTTX is the Passive Optical Network (PON). It is a point-to-multipoint fiber to the premises network architecture in which unpowered optical splitters utilizing Brewster's angle principles are used to enable a single optical fiber to serve multiple premises, typically 32 to 128. A PON consists of an Optical Line Terminal (OLT) at the service provider's Central Office (CO) and a number of Optical Network Units (ONUs) near end users. A PON configuration reduces the amount of fiber and CO equipment required compared with point to point architectures.

The telecommunications industry differentiates between several distinct FTTX configurations. The terms in most widespread use today are:

- FTTN / FTTLA (fiber-to-the-node, -neighborhood, or -last-amplifier): Fiber is terminated in a street cabinet, possibly miles away from the customer premises, with the final connections being copper. FTTN is often an interim step toward full FTTH and is typically used to deliver advanced triple-play telecommunications services.
- FTTC / FTTK (fiber-to-the-curb/kerb, -closet, or -cabinet): This is very similar to FTTN, but the street cabinet or pole is closer to the user's premises, typically within 1,000 feet (300 m), within range for high-bandwidth copper technologies such as wired ethernet or Institute of Electrical and Electronics Engineers, (IEEE) 1901 power line networking and wireless Wi-Fi technology. FTTC is occasionally ambiguously called FTTP (fiber-to-the-pole), leading to confusion with the distinct fiber-to-the-premises system.
- FTTP (fiber-to-the-premises): This term is used either as a blanket term for both FTTH and FTTB, or where the fiber network includes both homes and small businesses.
  - FTTB (fiber-to-the-building, -business, or -basement): Fiber reaches the boundary of the building, such as the basement in a multi-dwelling unit, with the final connection to the individual living space being made via alternative means, similar to the curb or pole technologies.

- FTTH (fiber-to-the-home): Fiber reaches the boundary of the living space, such as a box on the outside wall of a home. Passive optical networks and point-to-point ethernet are architectures that deliver triple-play services over FTTH networks directly from an operator's central office.

- FTTD (fiber-to-the-desktop): Fiber connection is installed from the main computer room to a terminal or fiber media converter near the user's desk.
- FTTE / FTTZ (fiber-to-the-telecom-enclosure or fiber-to-the-zone) is a form of structured cabling typically used in enterprise local area networks, where fiber is used to link the main computer equipment room to an enclosure close to the desk or workstation. FTTE and FTTZ are not considered part of the FTTX group of technologies, despite the similarity in name.

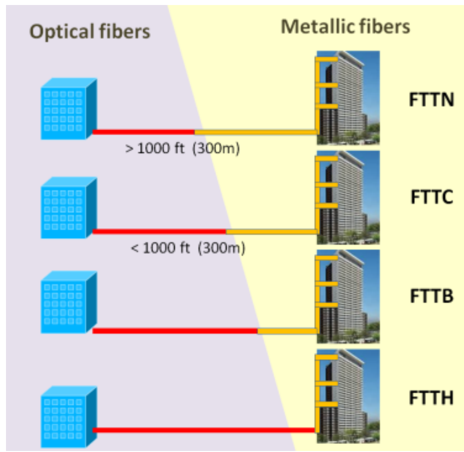


Figure 3-2-1. FTTX Access Networks

Increased competition from Multiple System Operators (MSOs), telcos, and IPTV service providers worldwide are driving the deployment of quadruple-play services over next-generation access networks. As a result, service providers are faced with many new business and service delivery challenges. New Optical Access Networks Delivering Higher Bandwidths for Increased Service Offerings.

Whether the access network is purely optical fiber-to-the home (FTTH) or based on a mixed fiber/copper technology (FTTC, fiber-to-the business (FTTB)), the requirements for operation and maintenance are changing dramatically compared to pure digital subscriber loop (DSL)-based access. At the same time, expectations have been set to reduce the maintenance effort especially on the fiber network, because it is regarded as more reliable than copper.

- XDSL (X Digital Subscriber Line)[17]

It is a family of technologies that allows access to provide broadband access network over conventional telephony (PSTN). Therefore, in the copper, the data are transmitted in a frequency range higher than that used for voice, while avoiding the mutual interference. Implementation of DSL modem requires placing a client at home and a team (called Digital Subscriber Line Access Multiplexer (DSLAM)) in the central operator. One of the main considerations in the deployment of this technology is the length of the local loop, as given band width varies inversely proportional to this length.

The example in the following Figure shows how the different access networks connect homes.

[17] ITU-T G Supplement 50 – Overview of digital subscriber line Recommendations; http://www.itu.int/en/ITU-T/studygroups/2013-2016/15/Pages/q4.aspx (2013-2016)

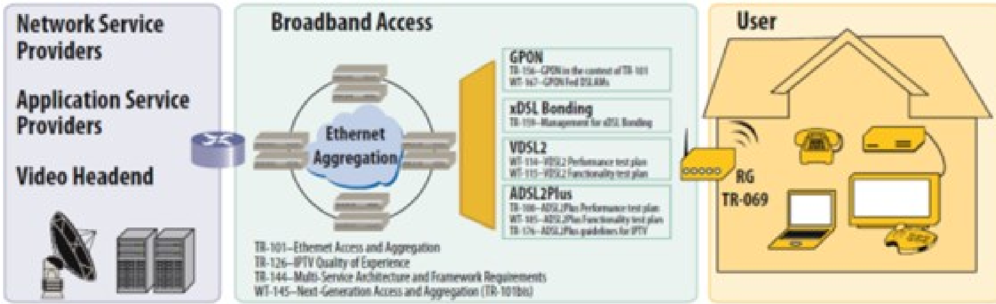


Figure 3-2-2. XDSL (X Digital Subscriber Line)

| Type | ITU-T | Initial approval | Max up/down |
|---|---|---|---|
| HDSL | G.991.1 | 1998 | 2 Mbps |
| ADSL | G.992.1 | 1999 | |
| SHDSL | G.991.2 | 2001 | |
| ADSL2 | G.992.3 | 2002 | |
| VDSL | G.993.1 | 2004 | |
| VDSL2 | G.993.2 | 2006 | 100 Mbps |
| G.fast | G.9701 / G.9700 | Dec 2014 / April 2014 | 1 Gbps |

Figure 3-2-2. DSL evolution

### 3.2.2. Passive Optical Network

- Overview

A PON is a telecommunications network that uses point-to-multipoint fiber to the premises in which unpowered optical splitters are used to enable a single optical fiber to serve multiple premises. A PON reduces the amount of fiber and central office equipment required compared with point-to-point architectures. A passive optical network is a form of fiber-optic access network.

In most cases, downstream signals are broadcast to all premises sharing multiple fibers. Encryption can prevent eavesdropping.

Upstream signals are combined using a multiple access protocol, usually TDMA.

A PON consists of a central office node, called an optical line terminal (OLT), one or more user nodes, called ONUs or ONTs, and the fibers and splitters between them, called the Optical Distribution Network (ODN). "ONT" is an ITU-T term to describe a single-tenant ONU. In multiple-tenant units, the ONU may be bridged to a customer premises device within the individual dwelling unit using technologies such as Ethernet over twisted pair, G.hn (a high-speed ITU-T standard that can operate over any existing home wiring - power lines, phone lines and coaxial cables) or DSL. An ONU is a device that terminates the PON and presents customer service interfaces to the user. Some ONUs implement a separate subscriber unit to provide services such as telephony, Ethernet data, or video.

An OLT provides the interface between a PON and a service provider's core network. These typically include:

- IP traffic over Fast Ethernet, Gigabit Ethernet, or 10 Gigabit Ethernet;
- Standard TDM interfaces such as Synchronous Digital Hierarchy (SDH)/ Synchronous Optical Networking (SONET);
- Asynchronous Transfer Mode (ATM) User Network Interface (UNI) at 155–622 Mbit/s.

The ONT or ONU terminates the PON and presents the native service interfaces to the user. These services can include voice (plain old telephone service (POTS) or voice over IP (VoIP)), data (typically Ethernet or V.35), video, and/or telemetry (TTL, ECL, RS530, etc.) Often the ONU functions are separated into two parts:

- The ONU, which terminates the PON and presents a converged interface—such as DSL, coaxial cable, or multiservice Ethernet—toward the user;
- Network Termination Equipment (NTE), which inputs the converged interface and outputs native service interfaces to the user, such as Ethernet and POTS.

A PON is a shared network, in that the OLT sends a single stream of downstream traffic that is seen by all ONUs. Each ONU only reads the content of those packets that are addressed to it. Encryption is used to prevent eavesdropping on downstream traffic.

- Variants of PON

(1) TDM-PON

For TDM-PON, a passive optical splitter is used in the optical distribution network. In the upstream direction, each ONU or ONT burst transmits for an assigned time-slot (multiplexed in the time domain). In this way, the OLT is receiving signals from only one ONU or ONT at any point in time. In the downstream direction, the OLT (usually) continuously transmits (or may burst transmit). ONUs or ONTs see their own data through the address labels embedded in the signal.

(2) DOCSIS Provisioning of EPON or DPoE

Data Over Cable Service Interface Specification (DOCSIS) Provisioning of Ethernet Passive Optical Network, or DPoE, is a set of Cable Television Laboratory specifications that implement the DOCSIS service layer interface on existing Ethernet PON (EPON, GEPON or 10G-EPON) Media Access Control (MAC) and Physical layer (PHY) standards. In short it implements the DOCSIS Operations Administration Maintenance and Provisioning (OAMP) functionality on existing EPON equipment. It makes the EPON OLT look and act like a DOCSIS Cable Modem Termination Systems (CMTS) platform (which is called a DPoE System in DPoE terminology).

(3) Radio frequency over glass

Radio frequency over glass (RFoG) is a type of passive optical network that transports RF signals that were formerly transported over copper (principally over a hybrid fibre-coaxial cable) over PON. In the forward direction RFoG is either a stand alone P2MP system or an optical overlay for existing PON such as GEPON/EPON. The overlay for RFoG is based on Wave Division Multiplexing (WDM) -- the passive combination of wavelengths on a single strand of glass. Reverse RF support is provided by transporting the upstream or return RF into on a separate wavelength from the PON return wavelength.

(4) WDM-PON

The multiple wavelengths of a WDM-PON can be used to separate ONUs into several virtual PONs co-existing on the same physical infrastructure. Alternatively the wavelengths can be used collectively through statistical multiplexing to provide efficient wavelength utilization and lower delays experienced by the ONUs.

- Advantages: The MAC layer is simplified because the P2P connections between OLT and ONUs are realized in wavelength domain, so no P2MP media access control is needed. In WDM-PON each wavelength can run at a different speed and protocol so there is an easy pay-as-you-grow upgrade.
- Challenges: High cost of initial set-up, the cost of the WDM components. Temperature control is another challenge because of how wavelengths tend to drift with environmental temperatures.

(5) Long-Reach Optical Access Networks

The concept of the Long-Reach Optical Access Network (LROAN) is to replace the optical/electrical/optical conversion that takes place at the local exchange with a continuous optical path that extends from the customer to the core of the network. This technology has sometimes been termed Long-Reach PON, however, many argue that the term PON is no longer applicable as, in most instances, only the distribution remains passive.

- Enabling technologies

Due to the topology of PON, the transmission modes for downstream (that is, from OLT to ONU) and upstream (that is, from ONU to OLT) are different. For the downstream transmission, the OLT broadcasts optical signal to all the ONUs in Continuous Mode (CM), that is, the downstream channel always has optical data signal. However, in the

upstream channel, ONUs can't transmit optical data signal in CM. Use of CM would result in all of the signals transmitted from the ONUs converging (with attenuation) into one fiber by the power splitter (serving as power coupler), and overlapping.
To solve this problem, Burst Mode (BM) transmission is adopted for upstream channel. The given ONU only transmits optical packet when it is allocated a time slot and it needs to transmit, and all the ONUs share the upstream channel in the TDM mode. The phases of the BM optical packets received by the OLT are different from packet to packet, since the ONUs are not synchronized to transmit optical packet in the same phase, and the distance between OLT and given ONU are random.

- Capacity Trend for PON

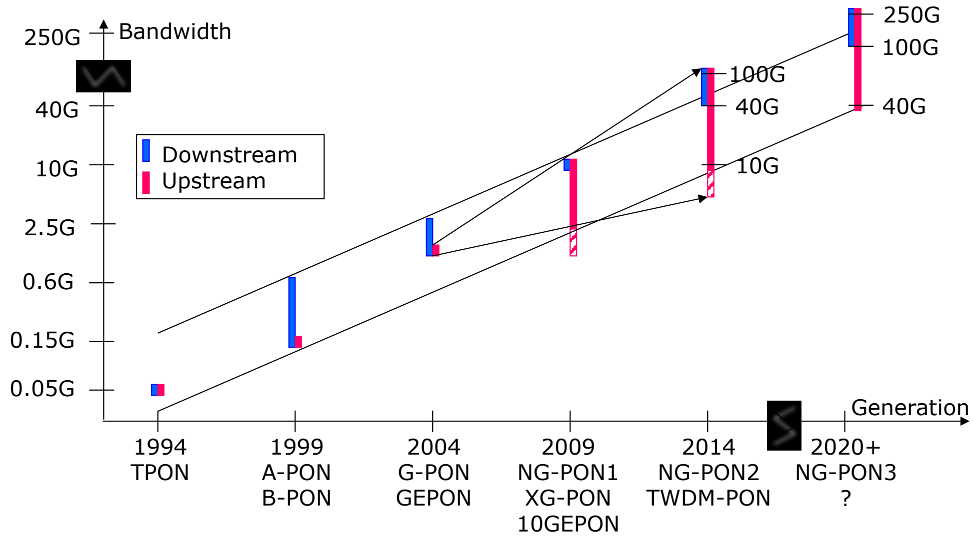



Figure 3-2-2. Source ITU-T SG 15 (October/2015)

### 3.2.3. Hybrid Fiber/Copper Networks[18]

- Fundamental types of hybrid fibre/copper (HFC) networks

An HFC network can be thought as composed of two main sections:

- First section: the "Transport Network" where the services are generated and delivered (at a national, regional or local level) up to main distribution points. The extension of the Transport Network can be huge. The physical transmission medium is the optical fibre.
- Second section: the "Access Network" where the final users are connected (at a local level) to the main distribution points. The extension of the Access Network is typically limited to a few kms in length. The bearer used in the first part of the Access Network is the optical fibre. The physical transmission medium of the last portion of the Access Network up to the users can be the symmetrical copper pair ("HFC-S" networks) or the coaxial copper/aluminium pair ("HFC-C" networks).

Typically, HFC-S networks are directly derived from traditional telephone copper access networks. The evolution towards new services can be achieved by means of particular data compression (for instance, Joint Photographic Experts Group (JPEG) and Moving Picture Experts Group (MPEG)) and transmission (for instance, High-bit-rate Digital Subscriber Line (HDSL), Asymmetric Digital Subscriber Line (ADSL), Very-high-bit-rate Digital Subscriber Line (VDSL)) techniques on the existing symmetrical pair cables.
The term HFC-C identifies a more restricted set of network solutions. HFC-C networks typically entail the installation of new active and passive coaxial components in the last portion of the Access Network, even if a simple update of an

[18] ITU-T L.47 (Access facilities using hybrid fibre/copper networks), ITU-T J.295 (Functional requirements for a hybrid cable set top box)

already existing HFC-C unidirectional network towards interactive services is considered. New HFC-C networks can offer up to 1 GHz bandwidth for CATV broadcast transmission and other broadband multimedia services.

- Guidelines for implementation

(1) HFC-S networks

HFC-S type identifies a wide set of very different network solutions, according to the level of the optical fibre penetration into the Access Network and to the network topology. So, installation procedures can involve a simple ADSL modem installation up to the in-field layering of new optical cables and ONU cabinets in the Access Network, with a huge variety of situations and potential problems.

It should be taken into account that:

- existing infrastructures should be used wherever possible (ducts, manholes, etc.);
- proper technical solutions should be studied in order to limit the environmental impact of new cabinets and new cable installation in terms of civil works, urban soil occupation, visual effect;
- proper technical solutions should be studied in order to ensure the reliability and the maintenance of the HFC-S network from the viewpoint of hardware and software;
- existing infrastructures should be studied as to how they could be reused in HFC-S networks.

(2) HFC-C networks

With respect to the HFC-S type, the HFC-C type identifies a more restricted set of network solutions. Some information and guidelines are given in the following on different HFC-C network elements.

- Coaxial cables

  Coax-trunk cables are typically less flexible and more cumbersome than, for instance, optical cables. Due to these reasons, ad hoc manholes, ducts and installation procedures have to be used in order to avoid any cable damage.

  It should be taken into account that:

  – suitable pulling, handling and layering procedures should be observed in order to avoid cable kinks according to the cable recommended curvature radius;
  – for in-duct installation, suitable ducts and manholes should be used for trunk cables. From 36 up to 63 mm diameter ducts have been reported for a single trunk cable installation;
  – for aerial or wall installation suitable cable accessories (holders, steel wires, lashes, etc.) should be used to support and fix the cable.

- Cabinets

  Suitable cabinet design should be carried out in order to ensure the operative range of active equipment according to their characteristics and to the environmental conditions (temperature, humidity, vibrations).

  Proper technical solutions should be studied in order to limit the environmental impact of cabinets in urban areas. Different cabinet versions for on-ground, underground and aerial installations should be studied in order to meet particular installation requirements.

- Indoor installation

  It should be noted that the installation of equipment for HFC-C networks in the customer's property could present problems in terms of obtaining permission of the user.

  It should be taken into account that:

  – existing building infrastructure should be used wherever possible;
  – additional infrastructure for drop cable installation should be avoided wherever possible;
  – cables and accessories have to satisfy country and regional regulations on fire protection requirements.

- General requirements

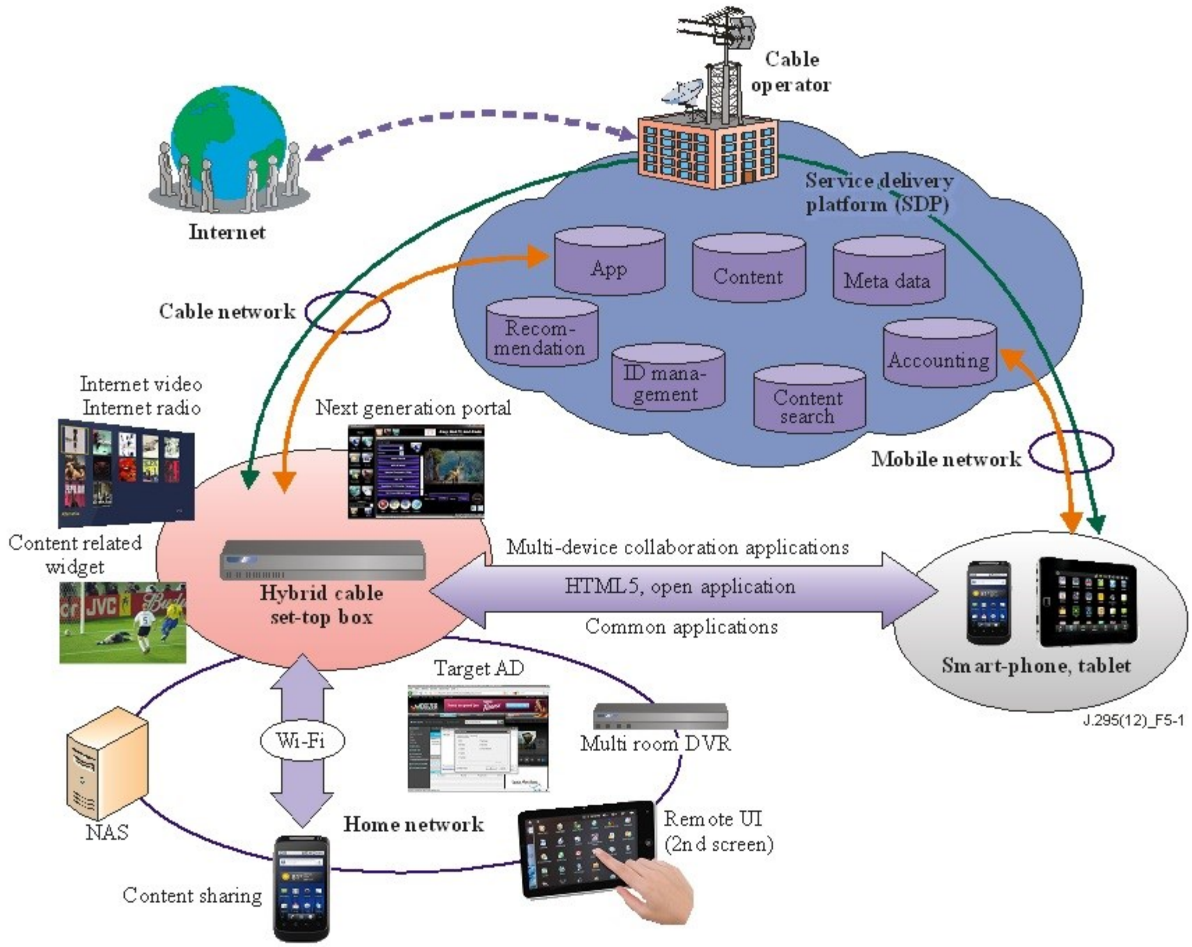



Figure 3-2-3. Overall cable architecture supported by the hybrid cable STB

Figure 3-2-3 illustrates overall cable architecture which consists of a service delivery platform, a cable network, mobile network, home network and the hybrid cable Set Top Box (STB) as a core device for advanced cable services. Figure 3-2-3 also shows some service aspects and the collaboration of applications based on this architecture.

The hybrid cable STB assumes the following conditions in the actual deployment stage.

- Services provided

  The hybrid cable STB is required to support cable integrated broadcast and broadband DTV services.

  The STB is required to receive terrestrial and satellite broadcasting re-transmitted (by trans-modulation) over an Radio Frequency (RF) (not over IP) on the cable access network. The STB is required to receive RF-based multichannel video programmes and can optionally support IP-based ones. The STB is also required to support interactivity such as Video on Demand (VoD), voice over IP, TV telephony and electronic commerce.

- Assumed cable network

  The network where the hybrid cable STB is to be used shall be the fibre to the home (FTTH), hybrid fibre/coax (HFC) or interactive coaxial network, which is currently provided by cable operators. The network is required to be a content delivery network managed by the cable operator. The network assumes interoperability with the networks provided by other operators (broadcasting networks, mobile phone networks, etc.). The network is required to have an Internet connection capability. Furthermore, it is required to connect with the home network inside the subscriber's residence.

- Cross platform

  The hybrid cable STB is required to provide services available not only on cable platforms but also on other platforms by coordination between the cable operator and other service providers operating those platforms.

- Open software

  The hybrid cable STB is recommended to apply open technologies as much as possible. Attention is drawn to possible IPR implications, e.g., consistency with the ITU-T Intellectual Property Right (IPR) policy and guidelines. Open-based operating system (OS), application programming interface (API), software development kit (SDK), etc. are recommended for the hybrid cable STB.

- Multi-tasking support

  The hybrid cable STB is required to support multi-tasking at the central processing unit (CPU) kernel level.

- CPU architectures

  The hybrid cable STB is required to not depend on any specific type of CPU architecture.

- Security

  The hybrid cable STB is required to be equipped with tampering check functions (including tampering prevention functions for the OS, firmware and middleware), application execution permission control, tamper resistance, etc. Enhancement of the CPU internal security is also required to protect it from software hacking by an open OS.

- Adaptation for technical evolution and compatibility

  The hybrid cable STB is required to support the cable application framework to ensure backward compatibility and also to support an open platform to prepare for future technical evolution.

- Service enhancement

  The hybrid cable STB is required to support service enhancement on the application layer.

- User interface (UI)

  The TV screen (first screen) and terminal device screen (second screen) are required to have the capability to support the various implementations of the UI. The UI is required to provide an intuitive operation for the user with minimum delay. The UI is required to have the capability to promote advanced services. Personalization and customization of the UI are required to follow the intention of the cable operator. The hybrid cable STB is required to enable subscribers to customize the UI within the permissions given by the cable operator.

- Cable portal

  The cable portal is the initial interactive presentation for the subscribers to access various services (TV broadcasting, VoD, web browsing, other interactive services, etc.) provided by the cable operator. It is required to enable the cable operator to customize the cable portal.

- Content protection

  It is required for the hybrid cable STB to be equipped with the conventional conditional access system (CAS) to protect broadcasting content. The hybrid cable STB is also required to support a conventional copy protection system already deployed in the cable industry. If content is re-distributed from the STB (e.g., to the home network) after the conditional access has been removed, the hybrid cable STB is required to apply the content protection method (e.g., Digital Transmission Content Protection (DTCP)-IP or higher capability) approved by the broadcasting industry.

- Home network connections

The hybrid cable STB is required to support IP network connections in the home network. The hybrid cable STB is required to support both the dynamic host configuration protocol (DHCP) server and client functions, logically. A Digital Living Network Alliance (DLNA) connection is required for video and audio content delivery within the home. The hybrid cable STB can optionally support connections to non-IP devices for various home appliances.

- Cable network architecture

The cable network architecture including the hybrid cable STB is shown in Figure 3-2-4. It is configured to distribute broadcasting and interactive services to the subscriber through the cable network where the transmission quality is guaranteed. However, if the source of the content is via the Internet, the quality cannot be guaranteed due to the best effort connection.

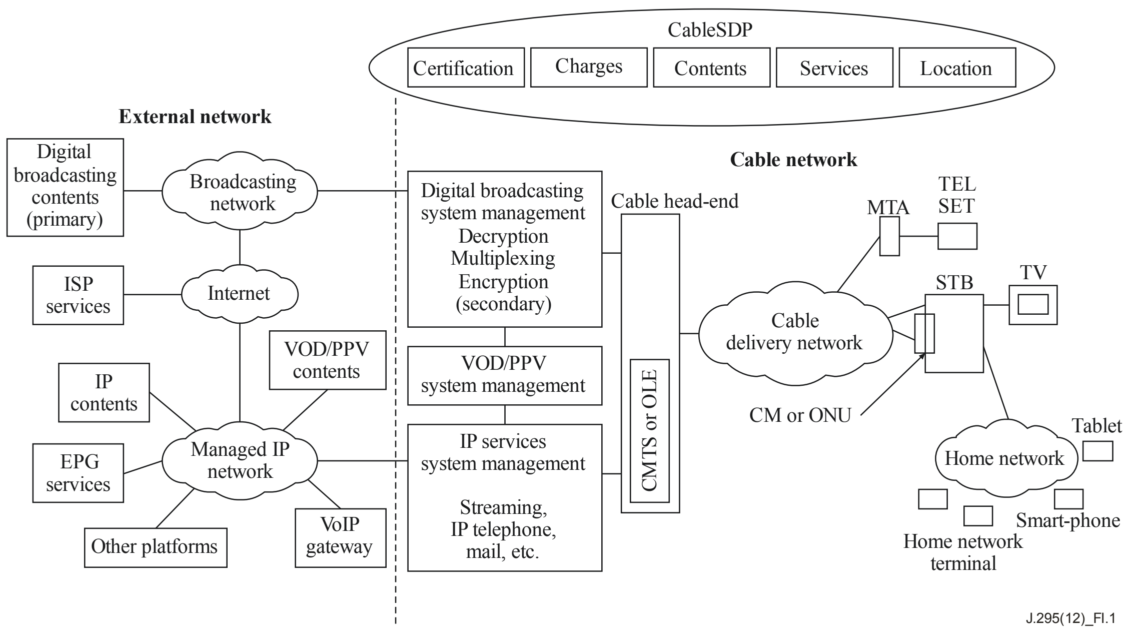



Figure 3-2-4. Cable network architecture

- Trend: G.fast/FTTdp: Fibre To The distribution point

One FTTdp architecture benefit is that the DPU equipment typically serves 1-20 lines, making it small enough to place on a pole, in a hand-hole or in a small pedestal.

A broadband access solution taking fibre to a distribution point (FTTdp) very close to the customers premises, with total wire length to the customers' transceiver up to 400m

FTTdp key aspects

- Provides the best of both worlds: Fibre to the home and ADSL
  - Fibre-to-the-home (FTTH) bit-rates
  - Customer self-installation like ADSL
- <u>Complements</u> FTTH:
  - Customer is unwilling to have his property excavated or interior redecorated to install fibre
  - Customers do not follow through with FTTH orders due to their unavailability or service issues
- <u>Enhances</u> FTTC:
  - Cabinets can move closer to the premises.

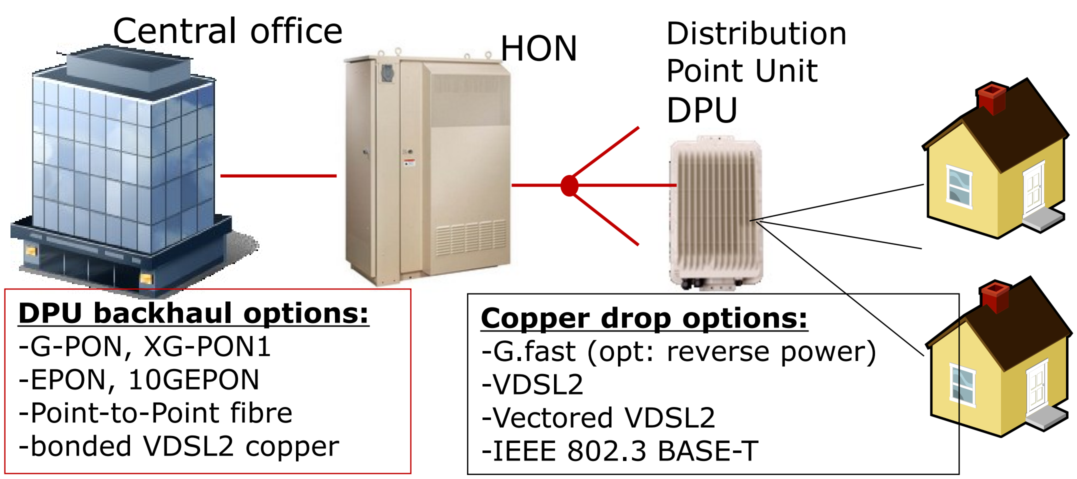



Figure 3-2-5. Source SG 15 (October/2015)

### 3.2.4. Fixed-Mobile Convergence General Requirements

International Mobile Telecommunications (IMT) systems are expected to provide users with access to a variety of advanced IP-based services and applications, supported by fixed and mobile convergence (FMC)[19] broadband networks, which are predominantly packet-based. The IMT-Advanced systems can support a wide range of data rates, with different quality of service requirements, proportional to user mobility conditions in multi-user environments.

- Objectives of Fixed Mobile Convergence (FMC)

The following points provide the general objectives for FMC:

- Seamless service operation from the end user perspective across heterogeneous fixed networks (i.e., PSTN, ISDN, PSDN, WAN/LAN/CATV, etc.) and mobile networks (i.e., GSM, CDMA2000, WiMAX, etc.), subject to any limitations imposed by the characteristics of the particular access technology being used.
- Seamless service provisioning from the service provider's perspective across heterogeneous fixed and mobile networks, subject to any limitations imposed by the characteristics of the particular access technology being used.
- Generalized Mobility defined in [ITU-T Y.2001] is supported in FMC (i.e., terminal device mobility, user mobility and session mobility). For a given scenario, different levels of mobility may be needed.
- Ubiquity of service availability where the end users can enjoy virtually any application, from any location, on any terminal device subject to any limitations imposed by the characteristics of the particular access technologies and terminal devices being used, given that the service has been subscribed.
- Support of multiple user identifier and authentication/authorization mechanisms.

- Fundamental characteristics of FMC

The following points describe the fundamental characteristics of FMC:

- Consistency of user experience is provided through a generic service delivery environment, which satisfies the needs of the fixed network and of the mobile network. The user is able to obtain services in a consistent manner as allowed by the connectivity and terminal device capabilities. Services are offered in accordance with FMC capabilities.

[19] This section is based on the Recommendation ITU-T Q.1762/Y.2802 (Fixed-mobile convergence general requirements).

- Subscriptions and service provisioning are access-technology agnostic but the service stratum may be aware of both the access and terminal device capabilities involved in a communication instance. Services are supported in all existing and emerging fixed and mobile access technologies where possible and subject to user preferences. Service registration, triggering and execution adapt to network and terminal device capabilities. The user's availability, reachability, and the terminal device's capabilities are perceptible to network functions, and as needed to services and applications, including those provided by a third party.
- FMC's service and application processing may depend on terminal device capabilities. Compatible terminal device capabilities may be selected by end-to-end interaction between terminal devices, or between the terminal device and the FMC service stratum according to the service and application needs.
- Support of generalized mobility, which includes service mobility, user, terminal device and network mobility. Reduced or partial mobility may be supported in some specific networks.
- A generic user profile for services which contains the criteria for session establishment and connectivity and is applicable both in fixed and in mobile networks, and which is specific to an individual user's subscription, containing, e.g., the user's address book, preferences, presence options, billing and payment options, service subscriptions and authentication parameters.

- Network environment

FMC needs to cover the possibilities for convergence across existing different network infrastructures and access mechanisms.

The following are among the envisaged network infrastructures:

- Fixed network, such as PSTN/ISDN, cable TV network, softswitch-based/IMS-based PES, IPTV service network, H.323[20] VoIP network and IMS-based NGN;
- Mobile network, multiple IMT-2000 family members consisting of the various releases of GSM evolved UMTS core network with UTRAN access network [ITU-T Q.1741][21], the various releases of ANSI-41 evolved core network with cdma2000 access network [ITU-T Q.1742][22], mobile WiMAX, etc.

The following are among the envisaged access mechanisms:

- The access network parts of IMT-2000: GSM/UTRAN and ANSI-41/cdma2000;
- WLAN in hot spots or as mesh networks;
- WiMAX broadband wireless access;
- xDSL, Cable, PLC, FTTH fixed access;
- Legacy PSTN systems used for narrow-band IP services access;
- The access network parts of digital audio broadcast (DAB) and digital video broadcasting (DVB)/digital video broadcasting handheld (DVB-H).

The following describes several scenarios for fixed-mobile convergence and indicate requirements associated with these scenarios.

- IP Multimedia Subsystem (IMS)-based FMC

  This convergence of fixed and mobile networks enables users to move between fixed and mobile access networks and still have access to the same set of IMS-based services. The fixed and mobile access networks might both be part of the user's home network, but it is a requirement that the case where one or both are visited networks is also supported.

- FMC between circuit-switched mobile and PSTN networks

  This convergence of fixed and mobile networks enables users to roam into the legacy PSTN network outside a GSM/UTRAN or American National Standards Institute (ANSI)-41/cdma2000 network. Limited mobility

---

[20] ITU-T H.323 v7, Packet-based multimedia communications systems, 2009

[21] Set of ITU-T Recommendations form Q.1741.1 to Q.1741.8

[22] Set of ITU-T rQ.1742.1 to Q.1742.11

is supported, e.g., nomadism, but service continuity (handover) is not required to be supported for this scenario.

- FMC in access network by UMA/GAN

  This convergence of fixed and mobile networks to enable the provision of service continuity for a multi-mode WLAN/2G terminal device when it changes its point of attachment is known as unlicensed mobile access (UMA). Demand for such capabilities is driven by competition on price and user convenience and the desire to extend service coverage in buildings with poor mobile radio reception.

### 3.2.5. Required Capabilities for Broadband Access for fixed mobile convergence[23]

- FMC service requirements

The following service requirements are defined.

- Access service support

  FMC is required to provide access-independent services for users.

  Also, FMC is required to offer to users the choice to select a suitable access transport to obtain service.

- Enhanced Virtual Private Network (VPN)

  Enhanced VPN service is an access-independent virtual private service network supporting multiple terminal types.

  Enhanced VPN makes it possible to provide a consistent virtual private network service by using a variety of public network resources, i.e., consistent VPN service across fixed networks, mobile networks and converged networks, and a variety of terminal devices.

  It is required to support the capability to allow users connecting to different public networks (i.e., PSTN, public land mobile network (PLMN), etc.). For this, it is required to support private network capabilities, such as use of a private numbering plan.

- Unified messaging

  Unified messaging means users can receive several types of messages, such as short message service, multimedia message service, instant messaging, e-mail, etc.

  FMC is required to let an end user choose the message type to be received. The end user may express message types to be received based on favourites, online state or terminal device type. FMC is required to support all types of messages from the sender and to transcode messages as far as possible into a format which the recipient is able to receive.

- FMC capability requirements

The following general requirements for FMC capabilities are defined:

- Access independence

  Services and features offered via FMC are required to be access-independent so that services are offered to users regardless of how they gain access.

- Uniform authentication and uniform authorization mechanism

  Due to the nature of FMC, FMC is required to provide a uniform authentication and a uniform authorization mechanism at the FMC service stratum applicable to any given configuration.

- Charging and management

  FMC is required to provide charging and management mechanisms.

---

[23] Relevant references on this topic are: ITU-T Q.1762/Y.2802 (Fixed-mobile convergence general requirements); ITU-T Q.1763/Y.2803 (FMC service using legacy PSTN or ISDN as the fixed access network for mobile network users); and ITU-T Y.2808 (Fixed mobile convergence with a common IMS session control domain)

- Service access environment

  FMC is required to provide the capabilities to access a wide range of application servers or service platforms. The underlying network may be circuit-based or packet-based.

- Quality of service

  FMC is required to provide QoS mechanisms.

- Interworking

  FMC is required to support interworking with existing networks, e.g., the legacy PSTN.

  Interworking does not impose any new requirements upon existing, non-FMC-capable networks other than to provide interfaces to interworking functions according to standardized mechanisms that are already supported by existing networks.

- Reliability requirements

  FMC is required to support reliable communications, including appropriate overload control and failure recovery mechanisms. The support of specific overload control and failure recovery mechanisms to manage and mitigate the consequences of such events to achieve the required level of reliability is not needed if the transport network and the processing systems are considered to yield sufficient reliability and are able to adequately mitigate overload situations.

- Security requirements

  FMC is required to provide security mechanisms to meet service requirements.

- Public services issues

  FMC is required to provide all the means to support public interest services required by regulations or laws of relevant national or regional administrations and international treaties. This includes requirements for:

  – lawful interception;
  – malicious communication identification;
  – unsolicited bulk telecommunications;
  – emergency telecommunications;
  – location information related to emergency telecommunication;
  – user identity presentation and privacy;
  – network or service provider selection;
  – users with disabilities;
  – number portability; and
  – service unbundling.

- Network selection

  FMC is required to support that a provider is able to define the preferred access network for service delivery in case the user has both fixed and mobile coverage. A user may indicate via the terminal device the preferred access network for access to services.

  The provider defines the policy regarding when handover between access networks is required to occur.

- Location identification

  FMC is required to support the ability to identify a user's location, and offers the location information to location-related services when the end user has given permission, and this is subject to public service requirements.

  The resolution of location information is dependent on the capabilities of the access technology.

  FMC is required to harmonize the different location identification mechanisms from existing networks.

- Personalized configuration

  FMC is required to support the ability to provide personalized services according to a user's requirement.

- Personal data network storage

FMC is required to store personal data on behalf of (or with permission by) the end user. It is required that the end user is able to access and manipulate those personal data through one of the user's various terminal devices.

- Accounting support capabilities

  FMC is required to support the ability to collect Call Detail Record (CDR) information from different network elements, which are used by the charging/billing system to gather together relevant usage data to initiate a unified bill to the specific user for multiple kinds of services with different terminal devices.

  In the case that the end user may be reachable by one identifier on different terminal devices, FMC is required to support to associate all relevant CDR information with the particular identifier.

- Message processing

  FMC is required to support the storage, transcoding, conversion and relay of different types of messages (SMS, MMS, IM, email, etc.).

- Presence information

  FMC is required to be able to store user presence information which can be accessed by appropriate applications.

- Mechanism for applications to access user data

  With permission given by the end user, FMC is required to provide mechanisms to enable applications to access relevant user data independent of where the end user data is stored.

- User identifier management

  An end user may have several different kinds of terminal devices, such as a legacy fixed terminal, a mobile phone, a personal digital assistant (PDA), a portable computer with extended capabilities, or a desktop fixed computer operating as a terminal with substantial multimedia capabilities.

  FMC has the ability to provide a unique user identifier at the transport stratum which allows differentiation among user terminal devices. Additional identifiers may be used at the service stratum to identify the user for end-user services.

  It is required to support user identification by:

– a single and unique identifier related to the user's subscription; or
– a number of such user identifiers mapped to a unique user identifier.

  FMC may apply a different end users' identifier when end user accesses different technologies, therefore Administrations or service providers may require common user identifier management to provide registration and authorization for the user regardless of the access mechanisms or terminals being used.

- Security capabilities

Access to the IMS session control domain and the services that are built on top of it does require the authentication and registration of users of this domain. Exceptions exist for emergency services.

Compared to stationary access in fixed networks, nomadic and wireless access in fixed networks and mobile access in mobile networks face an increased level of security threats. To counter these threats, a security framework has been adopted in the mobile world for IMS access, with the IMS subscriber identity module (ISIM) as a key component. The ISIM contains both user identity information as well as security mechanisms.

To facilitate FMC, it is recommended that the FMC terminal implements the ISIM functionality, to provide the same user identity information and the same level of security, regardless of whether the terminal is attached to a fixed or a mobile access. This Recommendation does not prescribe how the ISIM functionality is implemented. This may be in the form of a universal integrated circuit card (UICC), but other forms of implementation (e.g., "soft" ISIM) are not precluded.

- Public services capabilities

FMC may provide all the means to support public interest services required by regulations or laws of relevant national or regional administrations and international treaties. This may include requirements for:

- Lawful interception,
- malicious communication identification,
- unsolicited bulk telecommunications,
- emergency telecommunications,
- location information related to emergency telecommunication,
- user identity presentation and privacy,
- network or service provider selection,
- users with disabilities,
- number portability and
- service unbundling.

- IMS based FMC architecture

The high level FMC architecture is depicted in Figure 3-3-1. The architecture assumes a common IMS service platform for the delivery of services over fixed and mobile networks.

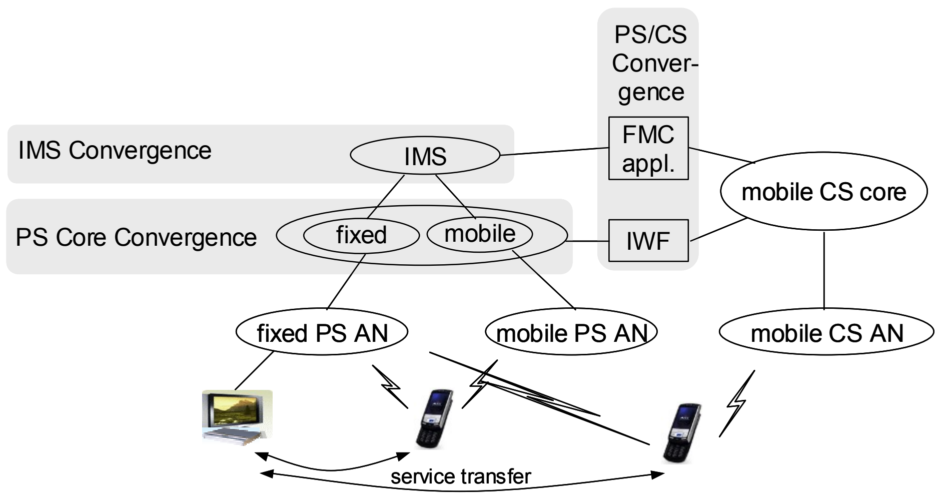



Figure 3-3-1. High-level IMS based FMC architecture

The converged IMS platform may be used to transfer services between terminals attached to different networks based on reachability, user preferences or at the user's explicit request. It may also be used to transfer services from one access to another access in order to provide service continuity for multi-mode terminals that can attach to both fixed and mobile access points.

- NGN domain model and convergence levels

(1) Principles of IMS-based service convergence

IMS-based service convergence enables a number of FMC service capabilities:

- Access to the same IMS-based services from different terminals using different public identities;
- Access to the same services from different terminals using the same public user identity;
- Service continuity on a multi-mode terminal whilst moving between a home or enterprise fixed network environment and the mobile network.

In terms of the domain model, the IMS-based FMC architecture is based on the following principles:

- The architecture is required to provide access to IMS-based services from any type of user equipment with IMS-compatible interfaces;

- the user equipment may be connected to any type of packet-based access transport domain with compatible interfaces that are able to convey the protocols between the user equipment and IMS transparently;
- access transport domains may be connected to a multi-access core transport domain, which implies that the interfaces between access and core may be access technology specific;
- the interfaces between the core transport domain and the IMS service platform are technology independent and based on the required functionalities to support IMS-based services and capabilities; this does not preclude the use of other service platforms that support this interface;
- the architecture is required to support sharing of access and core transport domain facilities by multiple service platform providers.

(2) Convergence levels

FMC functions can be viewed as functional elements that hide the difference between fixed and mobile access from the next higher level in the domain model and indirectly from the user. The location of the FMC functions determines the point/level at which the convergence takes place. The point of network convergence can be different among different network operators, depending on the nature of the current networks (mobile network, fixed network, Circuit Switched (CS) network, Packet Switched (PS) network, etc.). Figure 3-3-2 illustrates four possible points of convergence at different network levels (domains). Note that the access transport domains for fixed and mobile services are, per definition, different, although some common components may be shared between mobile and fixed networks. The same applies to core transport domains for mobile and fixed networks. A combination of all four types of convergence, as illustrated in Figure 3-3-2, may also be applied to allow for roaming between CS and PS domains, or to combine handover and service transfer capabilities.

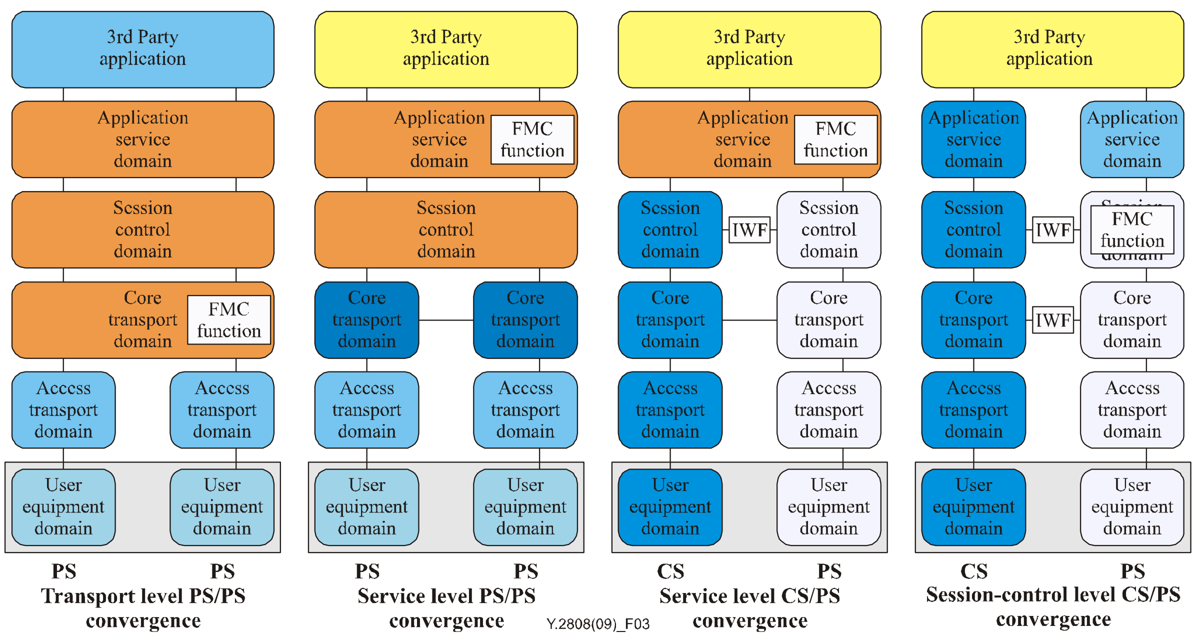



Figure 3-3-2. Convergence point and FMC function

### 3.2.6. Considerations for using legacy PSTN or ISDN[24]

The PSTN Access for Mobile users (PAM) service provides to mobile users access to voice and video telephony services utilizing the PSTN/ISDN via an available access point (AP) through an appropriate dual mode mobile terminal. Whether the AP is connected to the legacy network via a PSTN analogue or an ISDN access interface it shall

[24] For more information see ITU-T Q.1763/Y.2803 - FMC service using legacy PSTN or ISDN as the fixed access network for mobile network users. For deeper information on the fundamentals and requirements of packet-based networks see ITU-T Y.2600 series

not affect the service from the PAM user's point of view. In order words, the dual mode dual radio mobile terminal provides the user access to the legacy PSTN/ISDN networks and mobile networks using a single terminal.

- Service numbering

According to ITU-T Y.2803 the PAM service supports two types of numbering:

- The user is identified by a discrete PAM service number (referred to as a "fixed PAM service number" which may be in the form of, e.g., an UPT number). The fixed PAM service number is used separately from the user's mobile number (MSISDN). The fixed PAM service number is used to make and receive calls when the user is being provided service by means of a PSTN/ISDN access, while the mobile number (MSISDN) is used when the user is being provided service by means of a mobile network access.
- The user is identified by his MSISDN, which is also his PAM service number, independent of whether he is being provided service by a PSTN access or a mobile network access.

- Service subscription

The user needs to subscribe to the PAM service in advance.

- When the fixed PAM service number is used, the subscription information is as follows:
  - a fixed PAM service number assigned by the provider;
  - a user identity assigned by the provider which links to the PAM service number of the user;
  - the user's associated MSISDN for re-routing the terminating call to the mobile network in case the call is not possible to be completed through the PSTN/ISDN;
  - the service access code (SAC) of PAM service which corresponds to the PAM service controlling point of the home network.
- When a MSISDN is used as the PAM service number, the subscription information is as follows:
  - the user's IMSI;
  - a user identity assigned by the provider which links to the IMSI of the user terminal;
  - the service access code (SAC) of PAM service which corresponds to the PAM service controlling point of the home network;
  - the PAM service subscription to be registered in the user's service profile (in the HLR/AuC (HSS)).

- Registration and authentication for legacy fixed network access

The mobile user needs to register at a fixed network access point before making and receiving calls. Authentication is mandatory when a mobile user requests legacy PSTN/ISDN access.

## 3.3 Broadband Access for rural applications

Rural areas of countries continue to be sparsely covered and are not considered as a viable business case by telecommunication operators. Recent growth of teledensity in urban areas, fuelled by mobile technology, has meant that the digital gap between rural and urban areas has widened.

Rural populations need to be provided with mobile telephony and wireless broadband access, by connecting remote areas to the broadband core networks. Choosing efficient, cost-effective and fast-deployment technologies – whether wired or wireless networks – is the way forward to improve accessibility in those areas.

The key challenges for the provision of telecommunication services in rural areas are driven by both technological and economic considerations. Setting up backhaul connectivity remains a high-cost exercise. Erratic power supply or complete lack of energy sources is a major barrier, and photovoltaic power supply is increasingly becoming a viable alternative. The requirement to maintain sufficient backup systems raises operational costs substantially.

Several ITU activities contributes to the goal of digital inclusion, by providing assistance for the development of connectivity in rural and remote areas using suitable technologies for access, backhaul and sources of power supply[25].

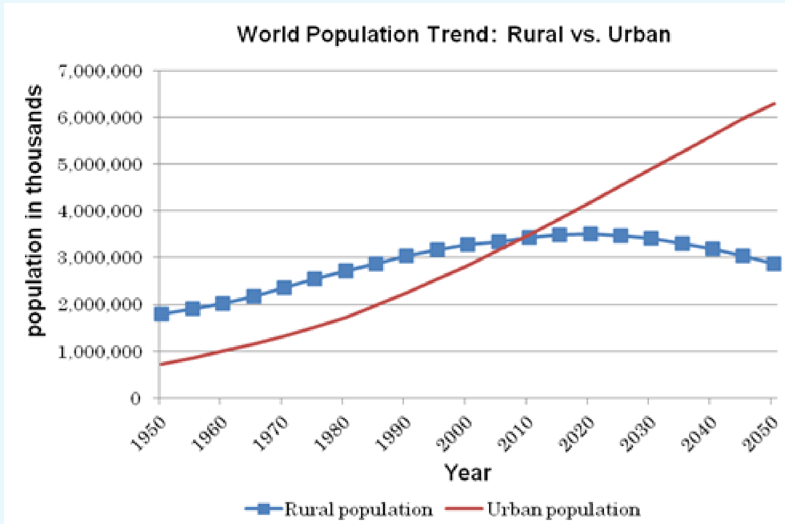
### 3.3.1. Overview

The World Summit on the Information Society (WSIS) (Geneva, 2003) Geneva Plan of Action sets the goal to provide internet available for all on this planet by 2015. Almost half of the global population is said to be in the rural areas according to the statistics of United Nation's Population Division (2009) as shown in Figure 1.

According to the Little Data Book (LDB) published 2012 by World Bank and ITU, there are globally over 6 billion mobile phone subscriptions, but 2/3 of the world's population still remain offline. Individuals using internet amounted to 2.4 billon and the number of fixed (wired)–broadband subscriptions reached almost 600 million. Broadband mobile penetration is limited. On the other hand, smartphone users are growing rapidly in developing countries. The challenges related to broadband infrastructure development in rural and remote areas are a reality in many countries.

---

25 ITU-D webpage on rural initiatives: http://www.itu.int/en/ITU-D/Technology/Pages/RuralCommunications.aspx




*Source: UNDP, 2009.*

Figure 3-3-1 – World Population Trend: Rural vs. Urban

### 3.3.2. Challenges for telecommunications/ICTs/broadband development in rural and remote areas

The WTDC-14 Recommendation D 20 [26] recommends that the state-of-the-art cost-effective techniques and technologies for broadband infrastructure development most suited for the geographical and economic conditions of rural and remote areas be put in place to enable these areas to access various e-applications, especially those which integrate them into national streams like e-governance, e-health, e-education, e-agriculture, etc. for vitalizing rural community through policy and regulatory interventions/initiatives

There are numerous challenges for the development of telecommunications/ICTs/broadband in rural and remote areas. These challenges have been presented from the perspective of the elements in entire telecommunications/ICTs /broadband ecosystem. The Final Report from ITU-D Study Group 2 Question 10-3/2 (2010-2014)[27] have identified the broadband value chain of stakeholders for promoting rural access, consisting of: governments, regulators, the telecom service providers, the customer premises equipment (CPE) manufacturers, the infrastructure manufacturer (vendors), the Value Added Service (VAS) providers, the content developers, the bilateral and multilateral donor agencies, the civil society organizations, the consumers.

---

[26] WTDC-14 Recommendation ITU-D 20, Policy and regulatory initiatives for developing telecommunications/ICTs/broadband in rural and remote areas.

[27] ITU-D Study Groups on Broadband access for rural applications and Final Reports:
- Question 5/1 (2014-2018): Terms of Reference http://www.itu.int/net4/ITU-D/CDS/sg/rgqlist.asp?lg=1&sp=2014&rgq=D14-SG01-RGQ05.1&stg=1;
- Question 10-3/2 (2010-2014): Telecommunications/ICTs for rural and remote areas: http://www.itu.int/pub/D-STG-SG02.10.3-2014;
- Question 10-2/2 (2006-2010): Telecommunications for rural and remote areas - Final Report http://www.itu.int/pub/D-STG-SG02.10.2-2010;
- New Technologies for Rural Applications, Final Report of ITU-D Focus Group 7, http://www.itu.int/ITU-D/fg7/pdf/FG_7-e.pdf (2000)

### 3.3.3 Backhaul and access for rural

The Final Report of Q 10-3/2 presents a comprehensive assessment of backhaul and access technologies for connecting rural and remote areas. Several technologies are covered with a view to tackle infrastructure challenges, such as: Optical access (e.g. P2P, PON, EPON, GPON and G.epon), optical backhaul (e.g. SDH, Carrier Ethernet and Ethernet on ROADM), terrestrial wireless technologies (Point-to-point vs. Point-to-muiltipoint), satellite-based solutions (e.g. FSS, NGSO, GSO), among others (see Figure 3-3-2).

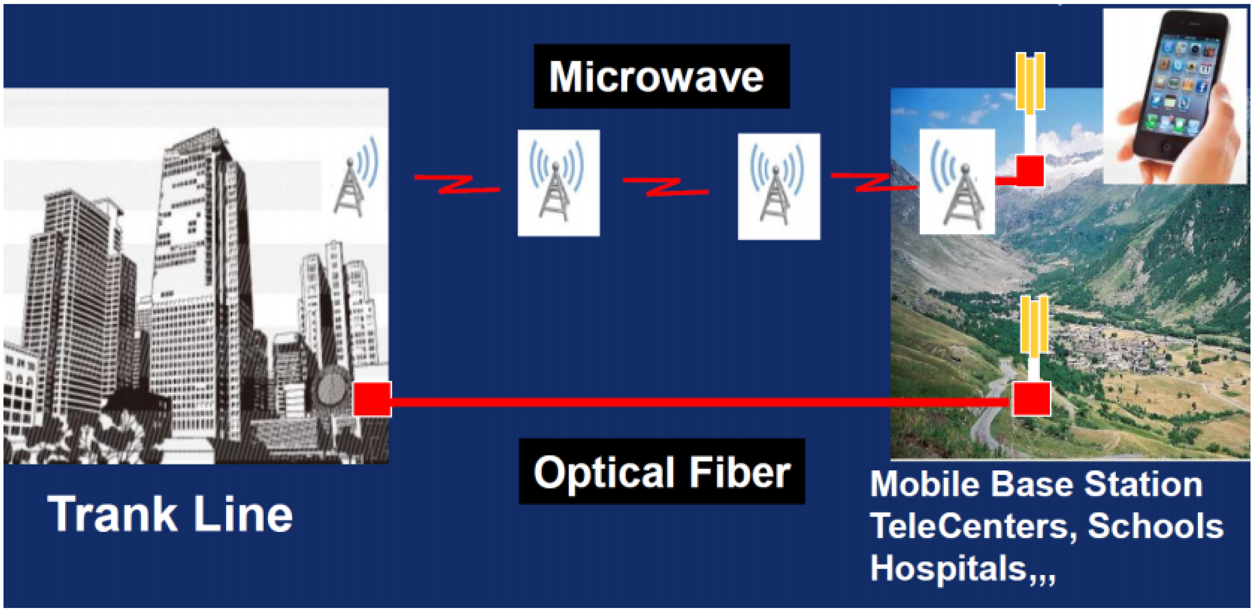



Figure 3-3-2 – Access challenge: broadband "backhaul" from cities to rural areas

The technology for appropriate infrastructure for broadband connectivity is broadly divided into wireless and wired technology. Out of the many options optical fiber stands out compared to wireless technologies that depend on availability of a rare resource like spectrum. Optical fiber offers enormous transmission bandwidths and high data rates. Using wavelength division multiplexing operation, the data rate or information carrying capacity of optical fibers can be enhanced to many orders of magnitude. The Transmission losses are low and can be further reduced to almost zero using ultra low loss fibers and the erbium doped silica fibers. However, laying fiber involves considerable upfront costs and takes time. A key concern is the difficulties in obtaining Rights-of-Way. The Satellite technology can be an alternative only in difficult terrains, in other areas cost would be much higher compared to that for optical fiber[28].

Given the diversity of the social, economic and geographical profiles of different parts of developing world, it is obvious that there is no uniform choice. It has to be a mix of wireless and wired backbone of services. What is more pertinent is over emphasis on competition among the service provider for efficient choice and use of technology. It is to be noted that competition may also lead to wasteful resource utilization. Service providers, in particular, build up infrastructure in competition to each other leading to more of the same problem. It is quite possible that through cooperation and partnership cost of infrastructure development could have been minimized to considerable extent. It requires an innovative regulatory framework to create an environment of cooperation as opposed to competition among the business enterprises.

In summary, backhaul for rural communications in developing countries should basically meet the following requirements:

[28] https://www.itu.int/md/D10-SG02-C-0158/fr

- Low CAPEX/OPEX
- Sufficient data capacity with future capacity upgradability
- Minimal need of Electric power
- Reliability under harsh environment and difficult terrain
- Safety against steeling, vandalism, small animal and natural disaster
- Installation and recovery with ease, speed and low cost
- Environmentally friendliness throughout the lifecycle with low energy consumption

### 3.3.4. ITU-D Case Study Library for Rural Applications

ITU-D Study Group Case Study Library allows members to submit, store and consult case studies on topics under study by the Questions in the ITU-D Study Groups[29]. Sharing and learning from each other's experiences is at the core of the mandate of the ITU-D Study Groups and through this new tool the remarkable wealth of information that are case studies will be available to all members. Improved features to search and filter have been put in place to make them more easily accessible.

[29] The ITU-D Study Group Case Study Library can be accessed on http://www.itu.int/en/ITU-D/Study-Groups/Pages/case-study-library.aspx

## 3.4 Core Networks

### 3.4.1. Overview

The deployment of core networks on a large scale has certain implications at the technology, economic and policy aspects[30]. In the technology aspect, specialized technical staffs are required for the deployment, operation and maintenance of this type of different sorts of network, including wireless networks[31]. In the economic aspect, demand for converging services has to be generated so that there is adequate use of the core networks. In the policy aspect, the policy and regulatory framework has to be appropriate and contribute to promoting the development of core networks.

After the implementation of NGN, enlarged capabilities in IP and underline transport with converged broadband capabilities will provide a way to support various services (e.g. IPTV, Cloud Computing, Smart Grid, etc.) over the common transport while keeping the simple linkage between Layer 3 and Layer 4.

NGN is a managed and converged network. The NGN core functions are responsible for ensuring information transport throughout the core network. They provide the means to differentiate the quality of transport in the core network. As such, many of the QoS techniques involving differentiated priorities and resource reservations, which are not widely applied in the Internet because of scalability and cost issues, can be applied within next-generation networks[32].

### 3.4.2. Key Areas for Core Networks

When considering the network and service evolution, the following key topics must be taking into account when setting up core networks[33].

- Quality of Service: IP network was originally designed for simple connectivity of best effort traffic. As the core network based on IP expands its capability to support various types of service, such as voice, video, and interactive games, the core network is required to support QoS.
- Decoupling of services and core transport: The decoupling of services and transport allows them to be offered separately and to evolve independently. Therefore in the core network, there shall be a clear separation between the functions for the services and those related to transport functions.
- Network management: With regards to network management, enhancement of the overall "core" network management architecture and definition of basic network management services and interfaces to suit NGN requirements (fault, configuration, accounting/charging, performance, security, customer administration, traffic and routing management).
- Generalized mobility: Generalized mobility means providing the ability of using different access technologies, at different locations while the user and/or the terminal equipment itself may be in movement allowing users to use and manage consistently their applications/customer services across existing network boundaries. In the future, mobility will be offered in a broader sense where users may have the ability to use more access technologies, allowing movement between public wired access points and public wireless access points of various technologies.
- Network control: Considering the increasingly distributed nature of the control functions, there is a need to provide network control systems supporting resource and QoS control, media processing, call/session control, etc.
- Interoperability of services and network: Considering that core networks will involve a large amount of protocols at the services and network level, there is a need to ensure the interoperability among systems and networks.

---

30 For strategies on migration to NGN see ITU-D SG2 Q26 Final Report - Migration from existing networks to next-generation networks for developing countries: technical, regulatory and policy aspect, 2014.

31 An example of a comprehensive set of standards covering core requirements for an IMT-2000 mobile network is presented by the ITU-T Q.1740 Series.

32 ITU-T Recommendation Y.2012 - Functional requirements and architecture of the NGN, release 1, 2006.

33 As defined by ITU-T Recommendation Y.2001 - General Overview of NGN, 2004. For more information on required capabilities for core networks see the ITU-T Y.2007 – NGN Capability Set 2. This recommendation provides descriptions of capability in terms of overall requirements and a high-level overview of the functional features to be addressed by NGN.

### 3.4.3. Technology and Deployment of Core Networks

- IP based Core Network

Modern digital technology allows different ICT sectors (e.g. wireline and wireless telecom) to be merged together. This convergence is happening on a global scale and is drastically changing the way in which both people and devices communicate.

At the centre of this process, forming the backbone and making convergence possible, are IP-based networks. IP-based systems offer significant advantages to operators and subscribers, from connectivity across a variety of devices, networks and protocols, to greater flexibility in management, use and cost of network resources. IP is the guarantee of openness for the beyond 3G/4G telecommunication network, which can merge data, voice and multimedia. Each component is able to handle IP protocols to provide transport for all types of bearer and signalling information in an All-IP network. However, the transformation of the current mobile network to All-IP network architecture cannot happen overnight. IP network is enlarging into the mobile network and fixed network gradually[34].

The prospective emerging mobile/wireless network, as noted in ITU-T Rec. Q.1702 and ITU-R Rec. M.1645, consists of diverse and different access systems and IP-based core network, such that the network can support interworking between these diverse access networks[35].

An individual user can be connected via a variety of different radio access systems to the networks. The interworking between these different access systems could be realized through a common IP-based core network with “optimally connected anywhere, anytime” manner. This IP-based core network shall be open to any service currently used and to be used in the future.

IP-based networks are classified into IPv4 and IPv6 according to the IP protocol types used[36]. Their behaviours differ according to the features of each protocol version. This principle to classify IP-based networks is also applied to differentiate instantiations of NGN, since it is based mainly on transport technologies employing IP technology.

IPv6-based NGN can be defined as a NGN which supports addressing, routing, protocols and services associated with IPv6. This applies not only to transport aspects in access and core networks but also includes other functions such as end user, transport control and application/service support functions in [ITU-T Y.2011] and [ITU-T Y.2012]. Taking into consideration these definitions and features, IPv6-based NGN could be identified as illustrated in Figure 3-4-4.

As shown in the Figure 3-4-4 below, there are three relationships among the NGN functions and Functional Entities in order to describe the IPv6-based NGN. First, there is a relationship between end-user functions and transport stratum. IPv6-based NGN allows flexible use of various access infrastructures to maximize the benefits of using IPv6. One such example is the use of multi-homing and mobility features, that is, IPv6-based NGN user terminal or equipment has a capability to handle multiple heterogeneous access interfaces and/or multiple IPv6 addresses through single or multiple access interfaces during the mobility between one network and the other. Second, there is a relationship between end-user functions and applications. IPv6-enabled end-user functions may acquire the information through application in order to support a secure and robust IPv6 transport. One such example is key management for IP security.

Finally, there is a relationship between the application and transport stratum. The application stratum could request the transport stratum to keep the high quality services. One such example is resource reservation.

[34] ITU-R Recommendation M.2114, “Key technical and operational characteristics for access technologies to support IP applications over land mobile systems,” 2007.

[35] ITU-T Recommendation Q.1703, “Service and network capabilities framework of network aspects for systems beyond IMT-2000,” May 2004.

[36] ITU-T Recommendation Y.2051 - General overview of IPv6-based NGN, 2008. A wide range of information related to IPv6-Based NGN standardization can be found at ITU-T Y.2050 series.

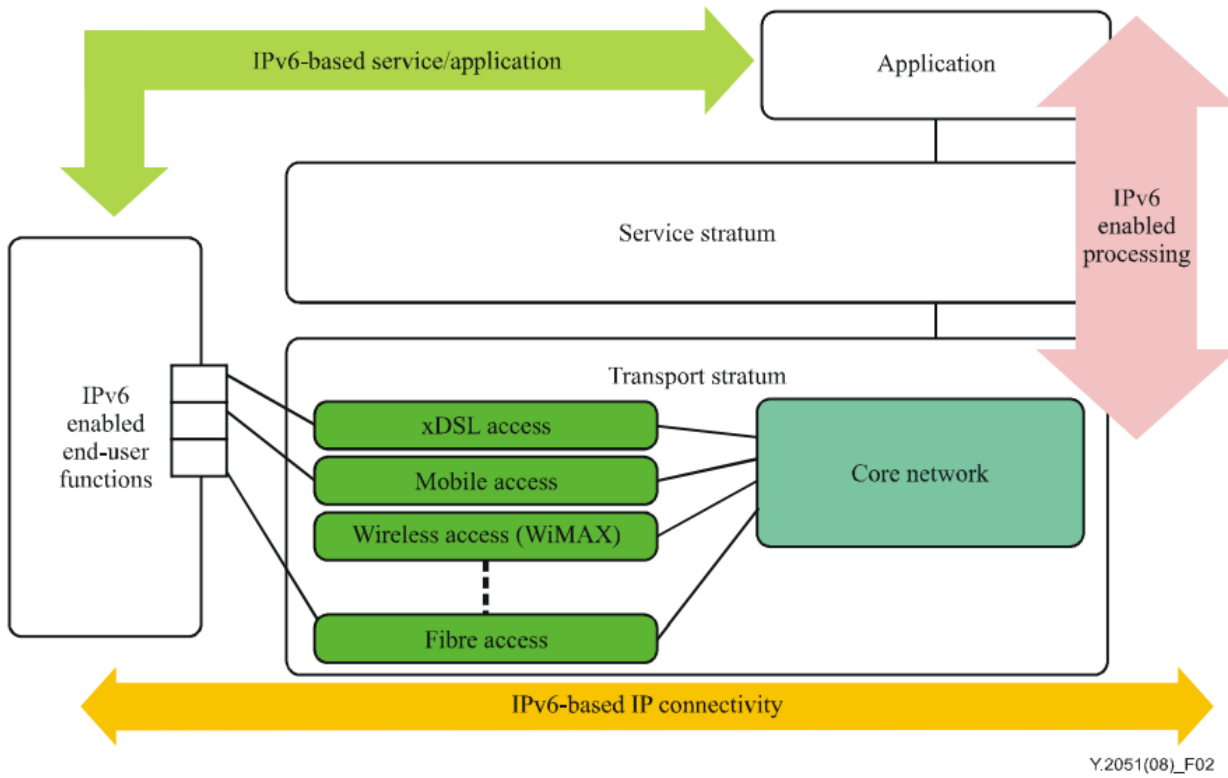



Figure 3-4-4 Overview of IPv6-based NGN

- NGN based Core Network

An NGN is defined by ITU-T as a convergent network platform based on the IP and horizontally integrated[37] and consolidating the technologies, network solutions and the electronic communication services such as data, voice, audiovisual content or other applications. It has a layered, packet mode architecture[38], facilitating the delivery of multiple services over a single infrastructure.

NGNs comprise two main elements: a next generation core and next generation access. The core network element is characterized by replacement of legacy transmission and switching equipment with IP technology in the core or backbone network.

The NGN network can be logically decomposed into different subnetworks, as shown in Figure 3-4-2. The emphasis on logical decomposition instead of physical decomposition is based on the fact that, in the future, physical equipment may have features of both the access network and the core network. A pure physical decomposition will encounter difficulties when such features are combined into a single network element.

[37] ITU-T Recommendation Y.1001, "IP framework - A framework for convergence of telecommunications network and IP network technologies," Nov. 2000.

[38] ITU-T Recommendation Y.2001, "General Overview of NGN," Dec. 2004.

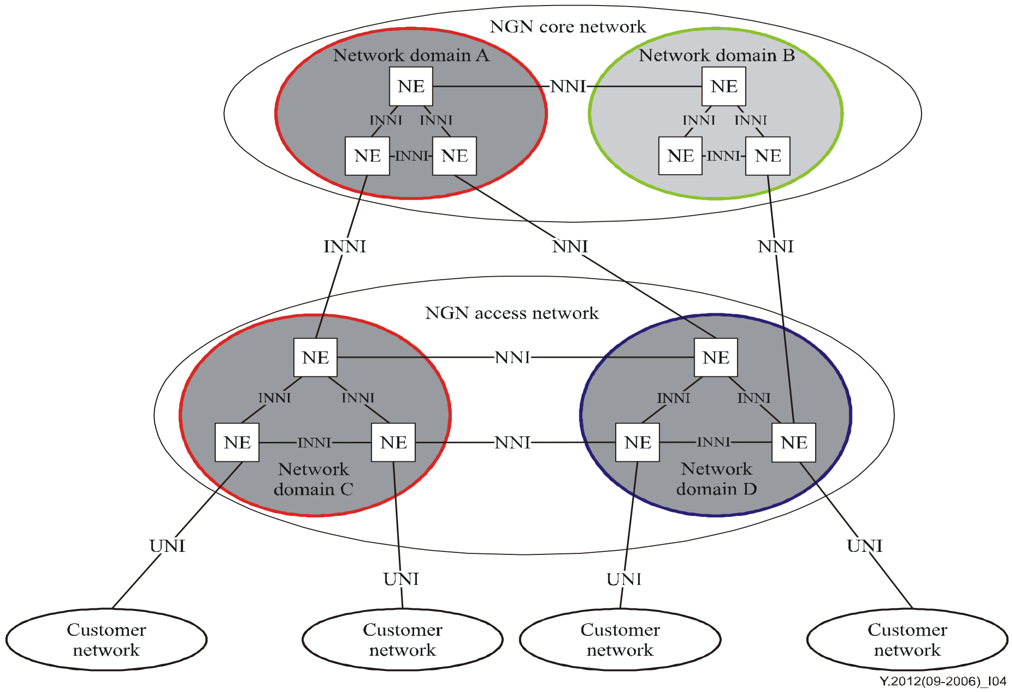


Figure 3-4-1 NGN interconnection at the network level

The major components of an NGN network are as follows[39]:

- End-user network: An end-user network can be a network within a home or an enterprise network. It is connected to the service provider's network via a UNI (user-to-network interface). The UNI is also the demarcation point between the service provider and the user.
- Access network: An access network collects end-user traffic from the end-user network to the core network. The access network service provider is responsible for the access network. The access network can be further partitioned into different domains, with the intra-domain interface being termed an INNI (internal network-network interface) and the inter-domain interface being termed an NNI (network-network interface). The access network belongs to the transport stratum.
- Core network: The core network belongs to both the transport stratum and the service stratum. The core network service provider is responsible for the core network. The interface between the core network and the access network or between core networks can be an INNI or an NNI.

The concept of an NGN domain is introduced to outline the administrative boundaries. Detailed topology information may or may not be shared across the NNI, but may be shared if available for INNI links.

On the other hand, it is also expected that a variety of the existing and new wired/wireless access network technologies are supported in NGN, as shown in Figure 3-4-2. Each of the access networks is connected to the NGN core network, to provide the same set of services for users, preferably independently of the access network type[40]. In this figure, the core network is that part of the NGN that provides the telecommunications and/or multimedia services of the NGN to the user. It is distinguished from the access network(s) in that it provides common functions shared across one or more access networks.

[39] ITU-T Recommendation Y.2012, "Functional requirements and architecture of the NGN release 1," Sep. 2006.

[40] ITU-T Recommendation Q.1706, "Mobility management requirements for NGN," Nov. 2006

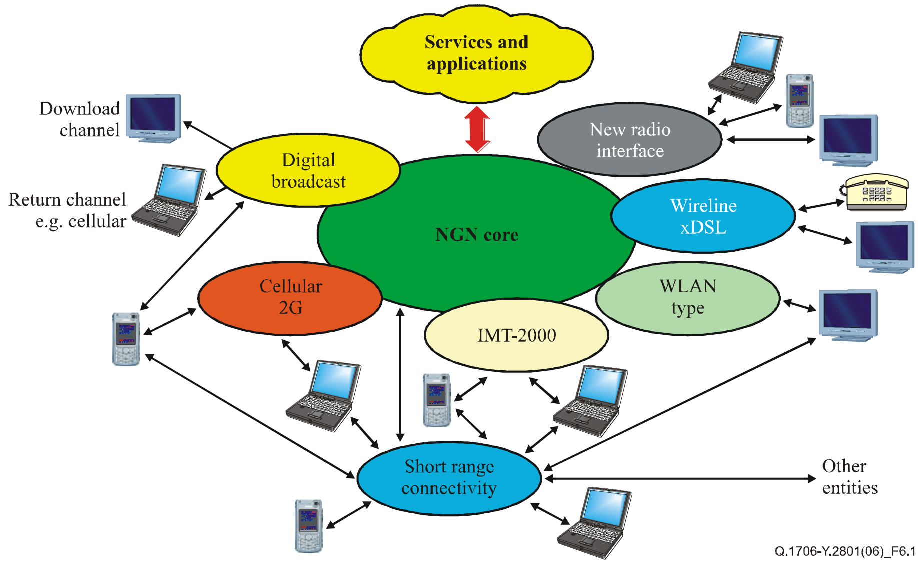



Figure 3-4-2 Envisioned network environment of NGN

- IMS based Core Network

IMS based core network is an architecture that offers multimedia services for users equipped with IP multimedia terminals.

IMS is a collection of core network functional entities for the support of SIP-based services [ETSI TS 123 228], [TIA-873.002]. IMS supports the registration of the user and the terminal device at a particular location in the network. As part of registration, IMS supports authentication and other security arrangements. The services supported by IMS may include multimedia session services and some non-session services such as Presence services or message exchange services.

In addition to services for the user, IMS defines a number of network reference points to support operator-provided services. IMS supports various application services via the services support architecture. IMS supports operation and interworking with a variety of external networks via defined reference points. IMS supports defined reference points for the collection of accounting data in support of charging and billing operations.

IMS also supports defined reference points within the underlying transport infrastructure for the enforcement of QoS negotiated by session signalling and for flow gating. These reference points also support the exchange of information in support of correlation of charging between IMS and the underlying transport[41].

The IMS is extended in NGN to support additional access network types, such as xDSL and WLAN. PSTN/ISDN simulation service is also provided by this component. In order to offer new multimedia services like IPTV, it is reasonable to reuse the well-established IMS-based core network infrastructure with Telco specific assets like guaranteed QoS, service interoperability or mobility.

The NGN IMS is comprised of a number of functional entities that together can provide support for the capabilities of the service stratum of NGN[42].

As shown in Figure 3-4-3, in the case of where PSTN/ISDN evolves directly to a NGN based on the IMS core network architecture, the end-users access the network using NGN user equipment or legacy user equipment connected via an access gateway[43].

[41] Recommendation ITU-T Y.2021, “IMS for Next Generation Networks,” Sep. 2006.
[42] ITU-T Recommendation Y.2012, “Functional requirements and architecture of the NGN release 1,” Sep. 2006.
[43] ITU-D Question 26/2 “Annexes to the main report on Question 26/2: Migration from existing networks to next generation networks for developing countries”.

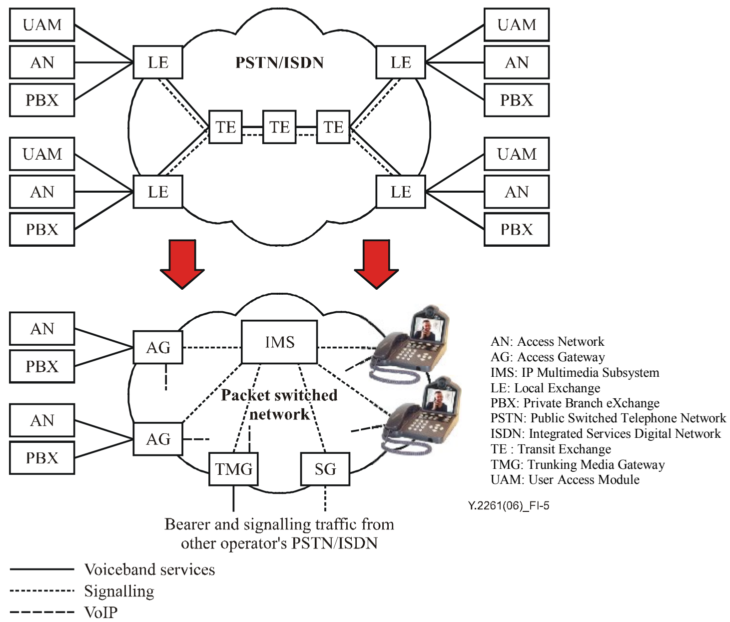



Figure 3-4-3 PSTN/ISDN migration to IMS-based core network

### 3.4.4 NGN interoperability testing

Interoperability testing for NGNs is performed on two or more products. Its objective is to check the ability and performance of the products implemented by mutually exchanging information. The interoperability testing procedures of described by ITU-T Q.3909 may be referred when undertaking NGN interoperability testing.

- Migration from existing networks to next-generation networks for developing countries: technical, regulatory and policy aspects

For further reference on NGN, the Report[44] from ITU-D Question 26/2 (Migration from existing networks to next-generation networks for developing countries: technical, regulatory and policy aspects) cover the following aspects, among others:

- Trends of telecommunication networks towards NGN;
- Examination of NGN technologies, Migration solutions to NGN (ITU-T SG13 works on NGN);
- Interconnection for NGN, technical and regulatory aspects.

[44] ITU-D Question 26/2 (2010-2014), Report: http://www.itu.int/pub/D-STG-SG02.26-2014

## 3.5 Home Networks

### 3.5.1. Overview

A LAN can be defined as a computer network that interconnects computers within a limited area such as a home, school, computer laboratory, or office building, using network media[45]. The defining characteristics of LANs, in contrast to WANs, include their smaller geographic area, and non-inclusion of leased telecommunication lines. Ethernet over twisted pair cabling, and Wi-Fi are the two most common technologies currently used to build LANs.

At the Data Link Layer and Physical Layer, a wide variety of LAN topologies have been used, including ring, bus, mesh and star, but the most common LAN topology in use today is Ethernet protocol. At the higher layers, the Internet Protocol (TCP/IP) has become the standard. Simple LANs generally consist of one or more switches. A switch can be connected to a router, cable modem, or ADSL modem for Internet access. Complex LANs are characterized by their use of redundant links with switches protocols, like the spanning tree protocol, to prevent loops and sometimes offering certain degree of management capable to differentiate traffic types via QoS or establishing VLANs.

A home network or home area network is a type of LAN that develops from the need to facilitate communication and interoperability among digital devices present inside or within the close vicinity of a home. Devices capable of participating in this network often gain enhanced emergent capabilities through their ability to interact. These additional capabilities can then be used to increase the quality of life inside the home in a variety of ways, such as automation of repetitious tasks, increased personal productivity, enhanced home security, and easier access to entertainment[46].

One of the primary drivers behind the establishment of this kind of network is the need to distribute residential Internet access to all Internet capable devices in the home. Due to the effect of IPv4 address exhaustion, most Internet service providers provide only one access-facing IP address for each residential subscription. Therefore most homes require a device capable of network address translation (NAT) that can route packets between the public address visible to the access network and private addresses of individual devices that share that public address. This router defines the boundary at which the service provider's network stops and the home's network begins.

Once a home network is connected to an access network, mechanisms need to exist that allow the network operator to manage fault, performance, transfer capability, addressing and security for the home network. In many cases, these will be the same as those used to manage the access network.

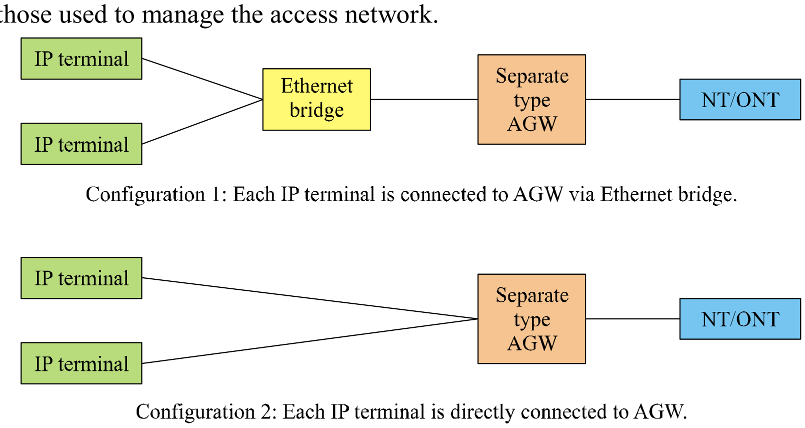



Figure 3-5-1 Example of typical IP home network configurations

Figure 3-5-1 shows two kinds of IP home network configuration. Configuration 1 shows that one Ethernet bridge either aggregates the traffic from multiple IP terminals to the access gateway (AGW) or bridges the traffic between two IP terminals. On the other hand, configuration 2 shows that each IP terminal is directly connected to the AGW[47].

---

[45] See definition in section 3.3.1 of this Report.

[46] Source: Adapted from Wikipedia, http://en.wikipedia.org/wiki/Home_network.

[47] ITU-T Recommendation G.9971, “Requirements of transport functions in IP home networks,” 2010.

Figure 3-5-2 shows major standardization bodies related to the home network.

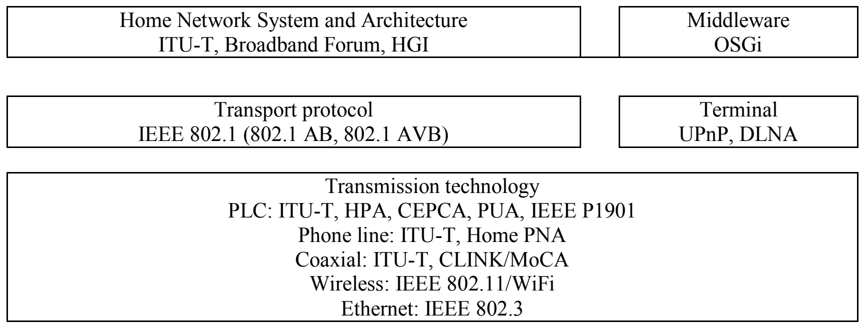



Figure 3-5-2 Major standardization bodies related to home network

Moreover, Figure 3-5-3 shows the relationship among existing study groups for home network within ITU-T.

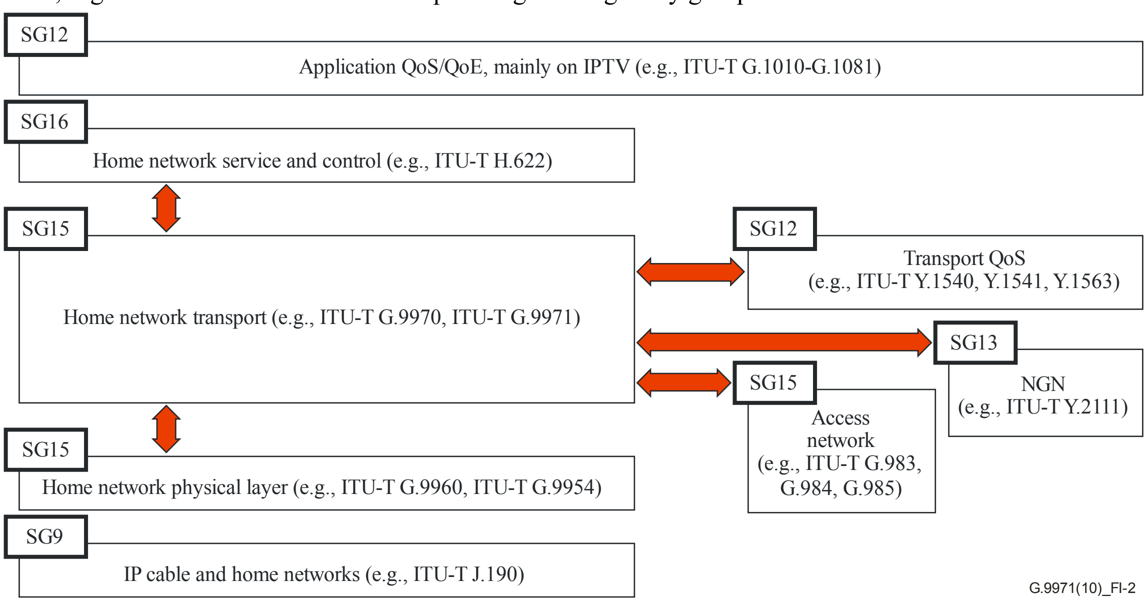



Figure 3-5-3 Relationship among existing ITU-T study groups for home network

### 3.5.2. Required Capabilities for Next Generation Home Networks

Next generation home network (NGHN) aims at providing the following characteristics[48]:

- Packet-based transfer, in particular support of IP as the protocol used at layer 3 in NGHN;
- User access to a wide range of services and applications (including real time/non-real time and multimedia services);
- Seamless environment for acquiring, sharing, storing and accessing digital media and content within the home network;
- Use of multiple broadband (wired and/or wireless), QoS-enabled transport technologies;
- Support of fixed and mobile terminals, including support of legacy terminals (e.g., PSTN/ISDN terminals);
- Automatic discovery and management of terminals attached to the home network.

- Energy saving using smart objects in home networks

---

[48] These requirements are defined by ITU-T Recommendation Y.2291, "Architectural overview of next generation home networks," 2011.

A considerable portion of energy consumed in our daily life is due to usage of home objects. To achieve energy efficiency, standards[49] have been developed to establish a set of minimum requirements and capabilities for saving energy by using smart objects in home networks.

In the ubiquitous network environment, everything is becoming connected. Figure 3-5-4 depicts energy saving using smart objects; it shows a diagram of home networks with examples of smart objects.

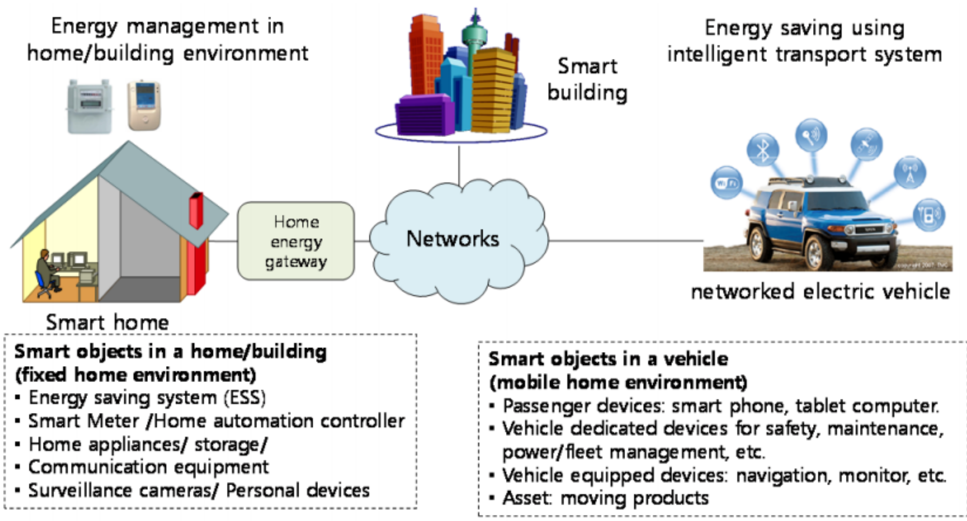



Figure 3-5-4 – Energy saving using smart objects in home networks

- Home Energy management system

The home energy management system (HEMS) [50] supports energy efficiency and reduction of the energy consumption. It is performed by monitoring and controlling the devices such as home appliances, storage batteries and sensors connected to the HN from the HEMS application.

While the algorithm for the energy efficiency and the reduction of the energy consumption runs in the HEMS application, the development of a standardized platform has been desired with the objective to provide common functions to enable the development and implementation of interoperable applications.

### 3.5.3. Architectural Overview of Next Generation Home Networks

NGHN provides two types of connectivity (Figure 3-5-5):

- Intra-home connectivity covers the connectivity of terminals within the home network. This includes connectivity of IP terminals at the home network terminal network interface (H-TNI) and connectivity of non-IP terminals via a non-IP gateway at the H-TNI;
- Connectivity to other networks covers the connectivity of NGHN at the UNI to other external networks such as NGN, non-NGN IP-based networks or PSTN/ISDN.

Considering these two types of connectivity, there are two major roles for the home network, i.e., extending the other networks (such as NGN) and their access network as well as interconnecting terminals in the NGHN itself. The portion working as an extension of the access networks must be aligned with the technical requirements of the network provider.

---

[49] ITU-T has approved the Recommendation Y.2064 - Energy saving using smart objects in home networks, 2014. Chapter 4.3.5 of this Report dedicates itself to the energy saving issues and ICT`s contribution.

[50] ITU-T Recommendation Y.2070 (2015) describes the reference architecture and the functional architecture the HEMS.

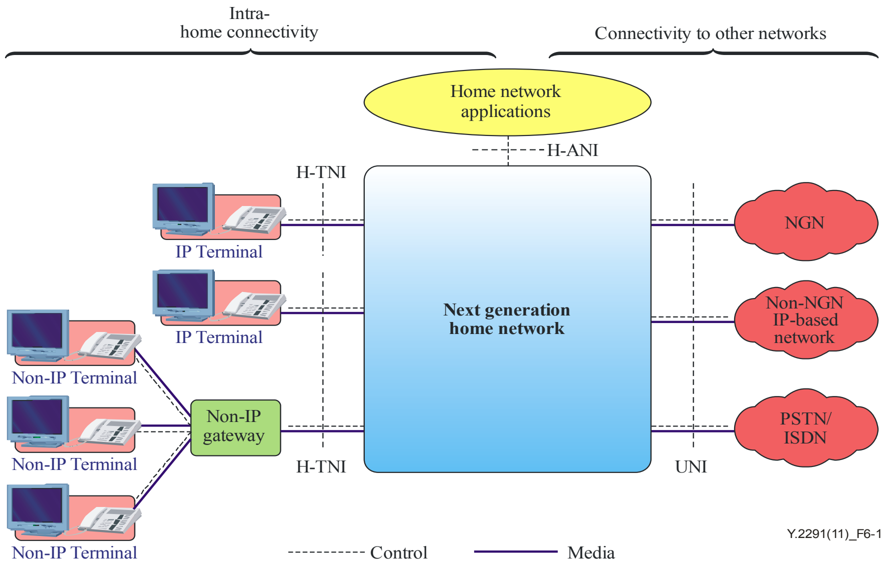


Figure 3-5-5 Connectivity to NGHN

The NGHN functional architecture supports the User Network Interface (UNI), H-TNI and home network Application Network Interface (H-ANI) reference points, shown in Figure 3-5-5.

The NGHN functions are divided into service stratum functions and transport stratum functions according to the principles described for NGN in [ITU-T Y.2011]. The NGHN service stratum provides the user functions that transfer service-related data and the functions that control and manage service resources and network services to enable user services and applications. The NGHN transport stratum provides the user functions that transfer data and the functions that control and manage transport resources to carry such data between terminating entities[51].

The delivery of services/applications to the end user is provided by utilizing the application support functions and service support functions and related control functions. The transport stratum provides IP connectivity services to NGHN users under the control of transport control functions within the NGHN, including the network attachment control functions (H-NACF), resource and admission control functions (H-RACF) and mobility management and control functions (H-MMCF). For the detail specification, refer to ITU-T Recommendation Y.2291.

[51] ITU-T Recommendation Y.2291, "Architectural overview of next generation home networks," Jan. 2011.

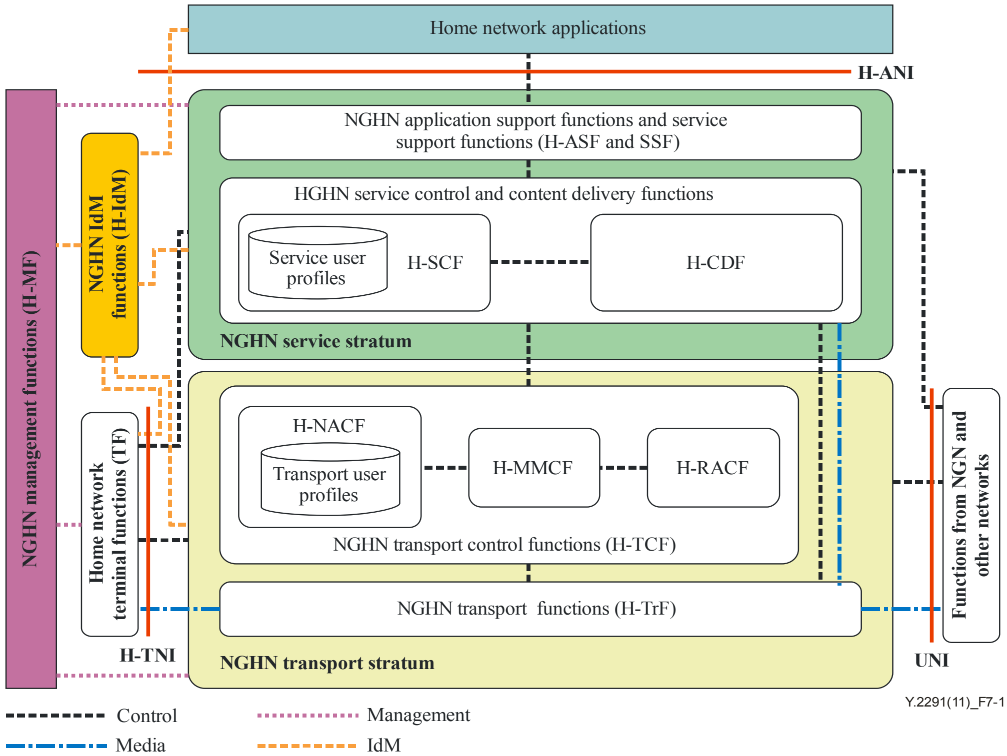



Figure 3-5-6 NGHN architectural overview

Figure 3-5-7 shows a configuration of a federation of NGHNs. The home network domain comprises heterogeneous home environments with NGHN functions. The NGHN functions support multiple different capabilities in accordance with needs of home network users and a federated configuration among multiple entities in the home networks.

The federation between multiple entities in the NGHNs creates physical, logical group environments or service/user community.

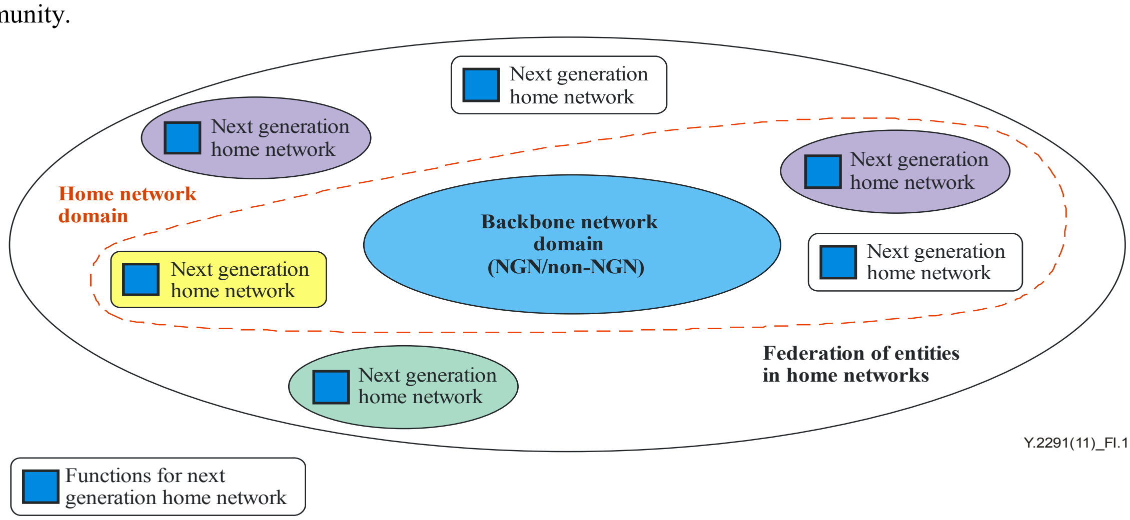



Figure 3-5-7 Configuration of a federation of NGHNs

## 3.5.4. Architecture and Deployment of Femtocells

Femtocells are low-power access points, providing wireless voice and broadband services to customers. They use fully standardised wireless protocols over the air to communicate with standard mobile devices, operating in licensed spectrum, generating coverage and capacity over Internet-grade backhaul. A typical deployment scenario is shown below[52].

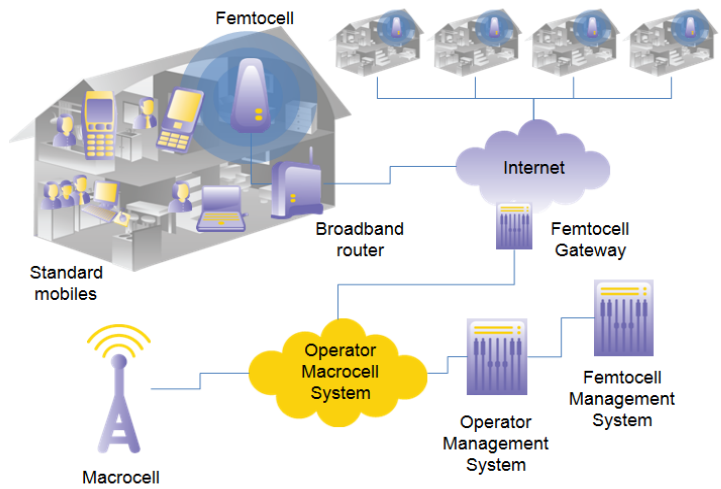



Figure 3-5-7 Typical femtocell deployment scenario

In the early stages of the femtocell industry, around 2007, there was a lack of standards for small cells and many femtocell vendors developed their own proprietary interfaces and network architectures for integrating femtocells into existing networks and addressing some of these challenges. Small Cell Forum attempted to gather all proposed femtocell architectures with the aim of distilling these into a single reference architecture. The result was the Forum's standard reference architecture model as shown in Figure 3-5-8. Small Cell Forum specified the main features of the architecture as follows:

- Femto Gateway (FGW) concentrates the connections of multiple Femtocell Access Points (FAPs) and presenting these to the existing core network as one connection. The FGW is therefore a "concentrator" of numerous femtocell connections so that the large volume of low power "Node Bs" or femtocells is not noticeable to the core network. Interfaces between femtocells and the core network are addressed by the FGW which acts as the translator between multiple femtocell specific IP based interfaces to a number of FAPs and a single interface to the core network.
- Security Gateway (SeGW) located in FGW sets up a secure connection between the FAP and FGW, provides authentication of the FAP and passes on operating parameters to the FAP based on decisions taken in the Femto Management System. FAPs are therefore securely connected to the core network without any additional signalling load on the core network.
- Femto Management System (FMS) provides the operation and maintenance of the FAP and potentially FGW including initial FAP setup, FGW discovery and setting of FAP operating parameters based on measurements reported by the FAP.

[52] Source: Adapted from Small Cell Forum, "Release One: Home Overview," Feb. 2013.

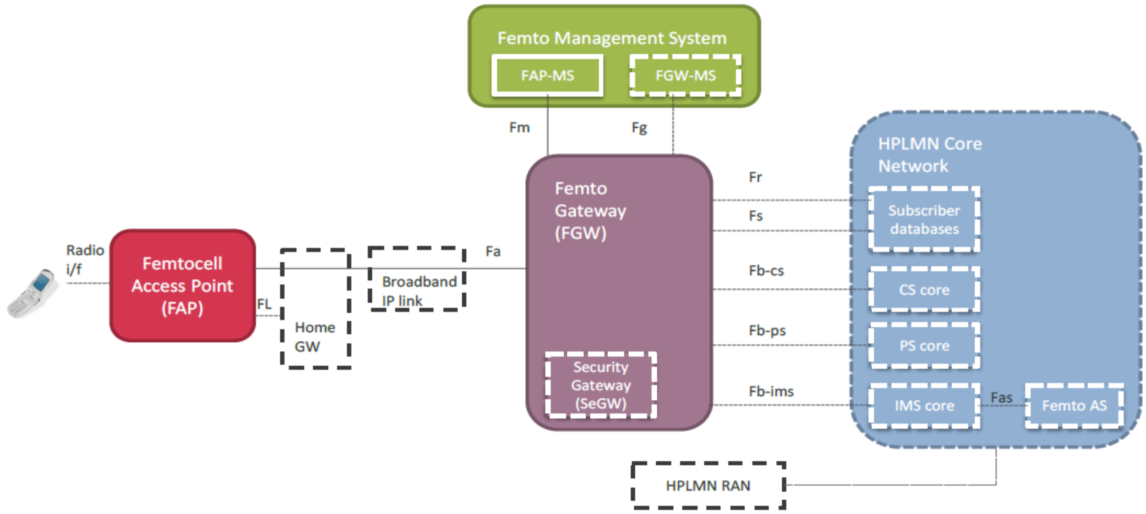



Figure 3-5-8 Small Cell Forum femtocells architecture reference model

## 3.6 Network Operation and Management

### 3.6.1. Overview

Many network operators and service providers have a large infrastructure of Operations Systems (OSs), telecommunications networks and equipment already in place, and which must be accommodated within the architecture in terms of managements. The objectives of the management is to facilitate the effective interconnection between various types of OSs and/or resources for the exchange of management information using an agreed architecture with standardized interfaces including protocols and messages. Management also provides capabilities for end-users with access to, and display of, management information, and end-user-initiated business processes.

Network operation and management requires agreement amongst suppliers and operators on the organization of processes amongst them that may be operated by people, OSs or other ICT systems. Based on generic network models for management, it is possible to perform general management of diverse equipment, networks and services using generic information models and standard interfaces.

Management of telecommunications networks is intended to support a wide variety of management areas, which cover the planning, installation, operations, administration, maintenance and provisioning of telecommunications networks and services. The ITU-T has categorized management into five broad management functional areas; fault management, configuration management, accounting management, performance management and security management[53].

### 3.6.2. Required Capabilities for Network Operation and Management

NGN management supports the monitoring and control of the NGN services and the service and transport resources via the communication of management information across interfaces between NGN resources and management systems, between NGN-supportive management systems, and between NGN components and personnel of service providers and network operators. NGN management supports the aims of the NGN by[54]:

- Providing the ability to manage, throughout their complete life cycle, NGN system resources, both physical and logical. This includes resources in the core network, access networks, interconnect components, and customer networks and their terminals.
- Providing the ability to manage NGN Service Stratum resources independently from the underlying NGN Transport Stratum resources and enabling organizations offering NGN end-user services to build distinctive service offerings to customers.
- Providing the management capabilities that will enable organizations offering NGN end-user services to offer customers the ability to personalize end-user services and to create new services from service capabilities.
- Providing the management capabilities that will enable organizations offering NGN services to provide end-user service improvements including customer self-service.
- Ensuring secure access to management information by authorized management information users, including customer and end-user information.
- Supporting the availability of management services any place any time to any authorized organization or individual.
- Supporting eBusiness Value Networks based upon concepts of business roles.
- Allowing an enterprise and/or an individual to adopt multiple roles in different value networks and also multiple roles within a specific value network.
- Supporting B2B processes between organizations providing NGN services and capabilities.
- Integrating an abstracted view on resources, which is hiding complexity and multiplicity of technologies and domains in the resource layer.
- Supporting the collection of charging data for the network operator regarding the utilization of resources in the network either for later use by billing processes (offline charging) or for near-real time interactions with rating applications (online charging).
- The ability to provide survivable networks in the event of impairment.

---

[53] ITU-T Recommendation M.3400, "TMN management functions," Feb. 2000.

[54] ITU-T Recommendation M.3060, "Principles for the Management of Next Generation Networks," Mar. 2006.

- The ability to have proactive trend monitoring.
- The ability to manage customer networks.
- The ability to have integrated end-to-end services provisioning.
- The ability to have automatic and dynamic allocation of network resources.
- The ability to have service quality-based network operations.
- The ability to have management that is independent of company organizations, which are subject to change, while maintaining the concept of organizational boundaries, and so on.

### 3.6.3. Management Architectures and Technology

Within the context of NGN, management functionality refers to a set of management functions to allow for exchanging and processing of management information to assist network operators and service providers in conducting their business efficiently. NGN management provides management functions for NGN resources and services, and offers communications between the management plane and the NGN resources and other management planes.

One of the architectural principles used in the management architecture for NGN is that of being a Service-Oriented Architecture (SOA). A SOA is software architecture of services, policies, practices and frameworks in which components can be reused and repurposed rapidly in order to achieve shared and new functionality. This enables rapid and economical implementation in response to new requirements thus ensuring that services respond to perceived user needs. SOA uses the object-oriented principle of encapsulation in which entities are accessible only through interfaces and where those entities are connected by well-defined interface agreements or contracts[55].

The NGN management plane is the union of the NGN service stratum management plane and the NGN transport stratum management plane following the basis of NGN functional architecture. Referring to Recommendation ITU-T Y.2011 as shown in Figure 3-6-1, NGN management plane places to cover both transport and service strata as well as other functions such as End-user functions.

NGN management functions provide the ability to manage the NGN in order to provide NGN services with the expected quality, security and reliability. These functions are allocated in a distributed manner to each functional entity (FE), and they interact with network element (NE) management, network management, and service management FEs. Further details of the management functions, including their division into administrative domains, can be found in [ITU-T M.3060/Y.2401].

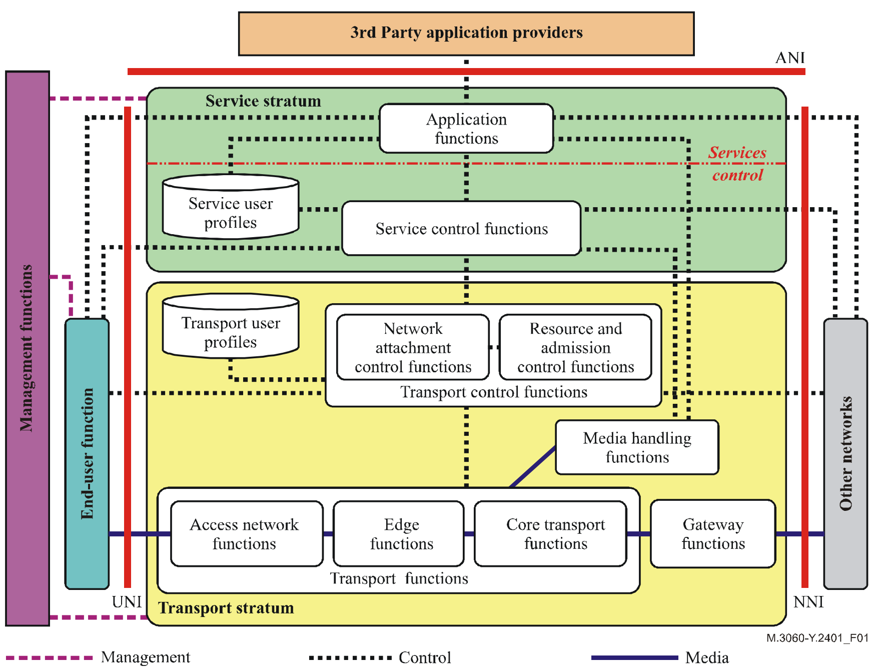



Figure 3-6-1 NGN architecture overview

[55] ITU-T Recommendation M.3060, "Principles for the Management of Next Generation Networks," Mar. 2006.

The NGN Management architecture will be divided into four different architecture views as shown in Figure 3-6-2 below:

- Business Process View: The business process view provides a reference framework for categorizing the business activities of a service provider.
- Management Functional View: The functional view permits the specification of what functions have to be achieved in the management implementation.
- Management Information View: The information view characterizes the management information required for communication between the entities in the functional view to enable the performance of the functions to be achieved in the management implementation.
- Management Physical View: The physical view describes the varied ways that management functions can be implemented. They may be deployed in a variety of physical configurations using a variety of management protocols.

Each view shows a different perspective into the architecture. Figure 3-6-2 describes the workflow in the creation of management specifications, where first the functional view is defined, followed by the information view and finally the physical view. The Business Process is an influence throughout the lifecycle. Note that, in practice, this process is iterative to enable all aspects of the architecture to evolve over time as required[56].

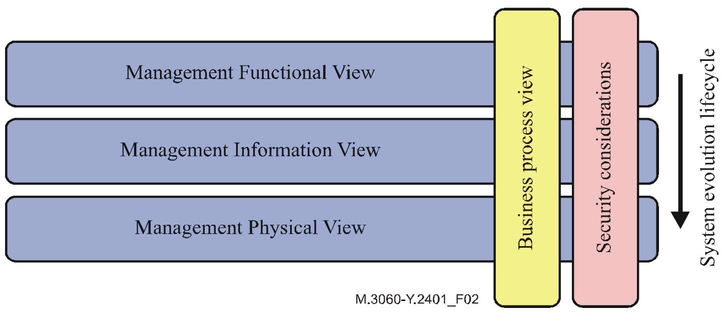



Figure 3-6-2 NGN management architecture

### 3.6.4. Accounting, Charging and Billing

The accounting, charging and billing interact with each other in the telecommunication infrastructure to collect accounting information in order to provide the telecom service provider with appropriate resource utilization data, enabling the service provider to properly bill the users of the system[57].

The accounting, charging and billing functions described in this clause are meant to represent a generalized architecture to support an NGN provider operator's need to collect and process information, such that customers can be charged for the services provided.

The charging and accounting functions (CAFs) provide accounting data to the network operator regarding the utilization of resources in the network. They support the collection of data for later processing (offline charging), as well as near-real-time interactions with applications, such as for pre-paid services (online charging). The CAFs include a charging trigger function (CTF), an online charging function (OCF), a charging collection function (CCF), a rating function (RF), and an account management function (AMF). Figure 3-6-3 shows the functions that comprise the CAF.

[56] ITU-T Recommendation M.3060, "Principles for the Management of Next Generation Networks," 2006.

[57] ITU-T Recommendation Y.2012, "Functional requirements and architecture of the NGN release 1," 2006.

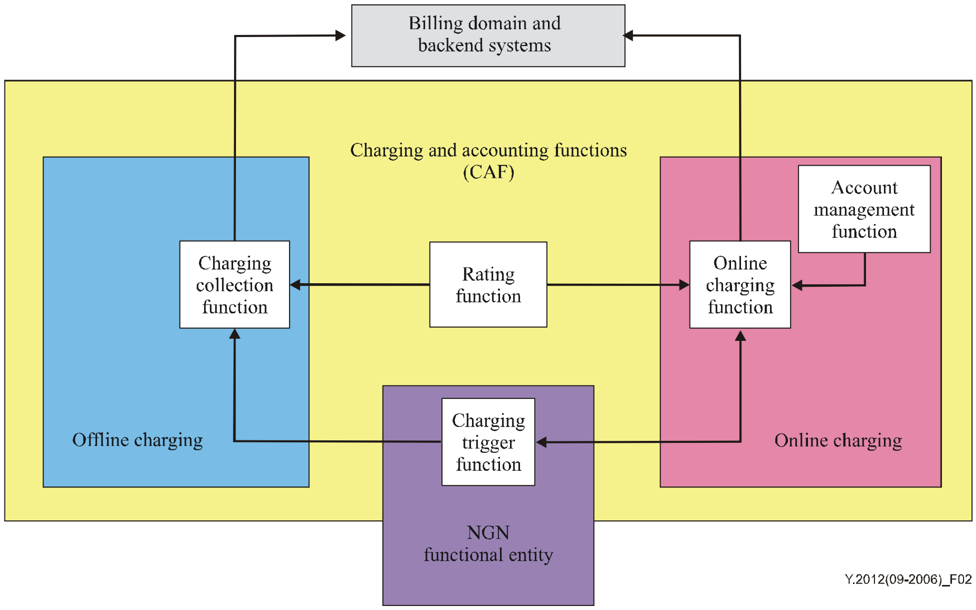



Figure 3-6-3 Charging and accounting functions

- Charging Trigger Function (CTF)

The CTF generates charging events based on the observation of network resource usage. In every network and service element that provides charging information, the CTF is the focal point for collecting information pertaining to chargeable events within the network element, assembling this information into matching charging events, and sending these charging events to the charging collection function. The CTF is therefore a necessary component in all network elements that provide offline-charging functionality.
The CTF also creates the charging events used for online charging. The charging events are forwarded to the online charging function (OCF) in order to obtain authorization for the chargeable event or network resource usage requested by the user. It must be possible to delay the actual resource usage until permission has been granted by the OCF. The CTF is able to track the availability of resource usage permissions during the network resource usage.

- Charging Collection Function (CCF)

The CCF receives charging events from the CTF. It then uses the information contained in the charging events to construct charging data records (CDRs). The results of the CCF tasks are CDRs with well-defined content and format. The CDRs are later transferred to the billing domain.

- Online Charging Function (OCF)

The OCF receives charging events from the CTF and executes in near real time to provide authorization for the chargeable event or network resource usage requested by the user. The OCF provides a quota for resource usage, which is tracked by the CTF. The OCF allows more than one user to share the same subscriber's account simultaneously. The OCF responds to the charging requests from various users at the same time and provides a certain quota to each user. The quota is determined by default or by certain policies. Users can resend requests for larger quotas during the same session.

- Rating Function (RF)

The RF determines the value of the network resource usage on behalf of the OCF. To this end, the OCF furnishes the necessary information to the RF and receives the rating output. The RF also works with the offline charging module, and it determines the value of the network resource usage.

- Account Management Function (AMF)

The AMF stores the subscriber's account balance within the online charging system. The subscriber's account balance could be represented by the remaining available traffic volume, time, or content, as well as money. Security and robustness can be emphasized by encrypting key data, providing backup and failure alarm capabilities, keeping detailed logs, and so forth.

## 3.7 Economic Aspects

### 3.7.1. Overview

Broadband has become a key priority of the 21st Century, and its transformative power as an enabler for economic and social growth makes it an essential tool for empowering people, creating an environment that nurtures the technological and service innovation, and triggering positive change in business processes as well as in society as a whole.

This economic impact of broadband manifests itself through different aspects (see Figure 3-7-1)[58]. The ITU-infoDev Telecommunication Regulation Handbook[59] highlights that broadband telecommunication infrastructure has the following impact on an economy:

- Positive contribution of broadband to GDP growth;
- Positive impact on productivity;
- Contribute to employment growth, both as a result of network construction programs and spill-over effects on the rest of the economy;
- The broadband has a positive effect on consumer surplus in terms of benefits to the end users that are not captured in GDP statistics. These benefits include efficient access to information, savings in transportation, and benefits in health.

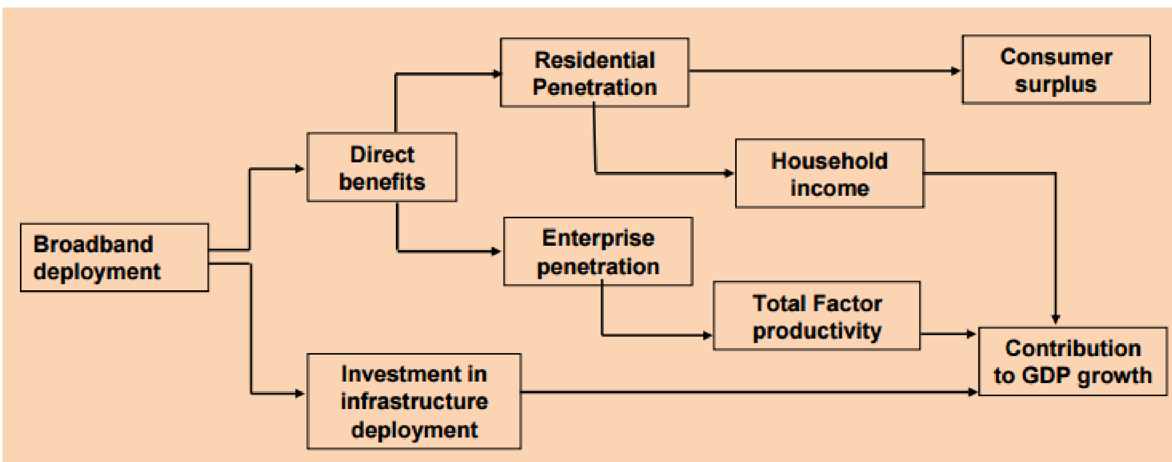



Figure 3-7-1. Broadband Economic Impact

In order to create economic conditions to implement IP applications and services, developing countries have, among other challenges, to put in place an enabling economic and regulatory framework that attracts both local and foreign investments and ensure their return on investment, and to identify many funding sources in order to invest massively in the rolling-out of IP infrastructures, applications and services, with benefits such as an increase of the national Gross domestic product (GDP) and job creation[60].

Driven by promises of reduced network infrastructure costs and increased productivity through converged applications, many organizations are deploying or evaluating the feasibility of IP communications. Various IP telecommunication services touch not only the telecommunication sector but the entire economy. Traditional operators need to co-operate with all market participants.

---

[58] ITU-D The impact of broadband on the economy, 2014

[59] For accessing the ITU-infoDev Telecommunication Regulation Handbook, see: http://www.itu.int/pub/D-REG-TRH.01-2011

[60] Adapted from the ITU-D Question 19-2/1 Final Report, "Implementation of IP telecommunication services in developing countries," 2014

When moving to broadband and converged telecommunication infrastructure, developing countries can obtain considerable economic and social benefits. In addition, given that telecommunication infrastructure allow access to voice, data and audiovisual content over a single carrier medium, it is important to envisage solutions aimed at enabling developing countries to significantly increase data exchange at national and international levels[61]. The economic and financial effects of the telecommunication infrastructure will vary according to the particular stakeholder including service provider or consumer.

### 3.7.2. Converged networks - Effects for Network Operators and Service Providers

Traditionally, telecommunications and broadcasting operated in separate, independent networks. With the advent of IP technology today it is possible for one operator to provide telephony, Internet, and broadcast services through one telecommunication infrastructure. Operational costs can be reduced by running a single converged network with common IP platform, rather than multiple networks[62].

Migration to broadband and converged telecommunication infrastructure including NGNs could change the operator's business models completely by reducing the time to market for new services, which can be brought to market faster and at lower cost. Operators would see much greater efficiencies and lower production costs, and might be able to develop new services in order to boost revenues and profitability.

Traditional PSTNs will come to the end of their normal economic life cycle; for example, the necessary hardware will become more difficult to find and more costly. IP-based telecommunication infrastructure is likely to be easier to operate and maintain than the existing legacy networks and provide the scope for operators with sufficient flexibility in their cost base to reduce both OPEX and CAPEX[63].

Market related convergence is also driven by consumer expectations, as they demand one-stop shop service, bundling of services and flat price packages. Increasingly, many service providers organize their tariff plans based on the volume of data transferred. Convergence is leading to increased competition in the markets as the same service is delivered through different infrastructure.

NGNs are a key enabler of fixed and mobile service convergence and essentially deliver convergence between the traditional world of PSTN and the new world of data networks. From an operator's perspective, NGNs provide a means of migrating from the old world to the new world of the "Information Society". They are making the convergence of fixed and mobile networks and the integration of voice and non-voice services their goals in response to consumer demand; such a market-based approach will lower operational costs and allow greater flexibilities for service innovation and increase their revenues.

### 3.7.3. Converged networks - Effects for Consumers

According to the researches of ITU Development Sector (ITU-D) Study Group Question 12-3/1, as various new services are provided by one service provider, the cost of providing services will be reduced compared to the provision of services separately. Therefore, consumers benefit from reduced prices. Converged services or bundled packages can be developed to improve the customer experience.

Consumers want more personalized services and better QoS. They also want simple invoicing systems reflecting all services used on the network as follows:

- Continuity: Changeover from PSTN to NGN is transparent to consumers, who will continue to use those PSTN services they are used to.
- Ease of migration: Consumers will be able to migrate seamlessly to new services offered by the same operator.
- Single access for multiple services: This will be enabled by the separation of the service layer from the network layer.
- Freedom of communication: Anytime & anywhere – Customers have access to suitable communication means in line with their requirements.

---

[61] Adapted from the ITU-D Question 12-3/1, "Tariff policies, tariff models and methods of determining the costs of services on national telecommunication networks, including next-generation networks," 2014

[62] Adapted from the ITU-D Question Final Report 19-2/1, ibid.

[63] Adapted from ITU-D Question 12-3/1, ibid.

- Innovative new services: New services will have richer functionality, and have a reduced time-to-market, since they exploit the distributed intelligence inherent in an NGN.

Migration to NGN enables consumers to choose their service providers and connection provider separately. They thus benefit from greater freedom and flexibility in choosing offers from different service providers and create their own "dynamic service package". This elimination of the intermediary ultimately creates further pressure on prices, which will force operators to seriously review their future business models and incorporate innovative aspects in their networks.

### 3.7.4 Enabling environment for ICT development

In order to assist the membership in the formulation, review and effective implementation of telecommunication/ICT policies, legislation and regulations, as well as allowing countries to make evidence-based policy and strategy decisions, ITU-D programme on policy and regulatory framework has delivered the following publications and have made them available on line for further consultation:

- annual publications on Trends in telecommunication/ICT Reform[64],
- the ICT regulation toolkit[65],
- the Broadband series of thematic reports[66],
- and the Regulatory and tariff policies database[67].
- a collection Best practices guidelines (2003-2014)[68] adopted at the annual Global Symposia for Regulator (GSR)[69].

It is worth mentioning that ITU-D Study Group 1, Question 1/1 (Study Period 2014-2018) is responsible for studying aspects of broadband policy and regulation, as well as broadband transition and implementation[70].

---

64 http://www.itu.int/pub/D-REG-TTR.14-2013

65 www.ictregulationtoolkit.org

66 https://www.itu.int/ITU-D/treg/publications/bbreports.html

67 http://www.itu.int/ITU-D/icteye

68 GSR`s discussion papers at http://www.itu.int/ITU-D/treg/Events/Seminars/GSR/index.html; and GSR best practice Guidelines at https://www.itu.int/en/ITU-D/Regulatory-Market/Pages/Events2014/GSR_award.aspx.

69 www.itu.int/bestpractices

70 ITU-D Q1/1 - *Policy, regulatory and technical aspects of the migration from existing networks to broadband networks in developing countries, including next-generation networks, m-services, OTT services and the implementation of IPv6*. Definition: http://itu.int/go/G7PN

## 3.8 Policy Aspects

### 3.8.1. Background

The development of ICT infrastructure is both a market and a regulatory challenge. An efficient policy regime can help the establishment of the infrastructure needed and extended to unserved areas[71].

Most developing countries started the telecom reform process much later than most developed countries. Now those countries are facing the daunting task of not just upgrading the national network for broadband access to Internet services but also extending the national telecom network to the population that has poor or no access to telecom services as well as to unserved rural areas.

The policy and regulatory environment has a heavy influence on both technical and economic opportunities. That environment can foster new opportunities or restrict, delay and sometimes even prevent them from being realized. Proactive regulation can foster the development and application of new technologies.

The primary challenge is to adopt appropriate policies and regulations that will facilitate the transition and growth of national telecom infrastructures that will ultimately support the overall development of e-economies and information societies[72].

### 3.8.2. Key Topics on Policy and Regulation

The following topics presents some of the policy and regulation challenges faced when defining ICT policies and regulations:

- **Regulation of Prices and Competition**

Price regulation in any market is most commonly used as a tool for competition drive. This is because, in the absence of price regulation, service providers with significant market power may increase prices beyond the levels they would do if the market was competitive. Another example would be the setting of prices that are anti-competitive.

Competitive telecommunications markets can serve consumers and the general economy better than regulation or other government intervention. One key reason is that setting prices and conditions of service aimed to benefit both service providers and customers requires large amounts of information, more than a single organization can easily gather, keep up-to-date and use. This is true whether the organization is from public or private sector. In competitive markets, changes to prices and conditions of services are generally made by trial and error, taking into account what has worked in the market and what has not. Competitive market forces can process more information more efficiently than any individual player.

The benefits obtained from competition is a key element for promoting efficiency and consumer welfare by inducing firms to produce more with less, better allocating resources, introducing new technologies, and meeting customer demands. In the Organisation for Economic Co-operation and Development (OECD) countries, markets with healthy levels of competition have led the introduction of innovative services and appealing pricing packages. Price decreases and improved services have been the most significant in markets characterized by intense competition[73].

- **Infrastructure Interconnection and Sharing**

With recent technological developments the range of services that depend on interconnection have increased. In addition to the more 'traditional' local, long distance, international fixed and mobile voice services, interconnection is also an essential input for satellite, Internet, e-mail, fixed and mobile broadband data transmission, and a wide range of multimedia services. Interconnection of communications networks is now routinely practiced across the globe, and convergence has accelerated the pace. Thus, networks operators have to deal with an expanding array of interconnection arrangements, which are widely recognized as beneficial to interconnecting carriers, consumers, and end users.

---

[71] ITU-D Question 12-3/1, "Tariff policies, tariff models and methods of determining the costs of services on national telecommunication networks, including next-generation networks," 2014.

[72] ITU-D Question 19-2/1, "Implementation of IP telecommunication services in developing countries," 2014.

[73] ITU Broadband thematic report, "Regulating Broadband Prices", 2012.

On the other hand, such interconnection and sharing arrangements are required by regulations in order to facilitate network access, ensure competition, and achieve gains in productivity. Regulatory frameworks must be developed to promote infrastructure sharing and to provide incentives for operators encouraging infrastructure interconnection, infrastructure sharing including access to facilities, while also stimulating investment. It is also important to hold public consultations on the various strategies and regulations for infrastructure sharing, with the participation of all the parties involved.

- **Transition to Emerging Telecommunication Infrastructure**

Transition to emerging telecommunication infrastructure through NGN calls for business models capable to conduct investment on a core IP network in combination with a range of available access technologies. In order to ensure a smooth transition, it will be necessary to review policy requirements as regards factors determining the choice of core and access technologies. Most developed countries have embraced NGN by adopting technology-neutral regulation, and developing countries can learn from such experiences when designing frameworks for transition to NGN.

An important challenge lies on actively contribute to and influence in the international standardization process to include the capabilities required for the roll out of NGN networks and growth of the data communications within their environs[74].

According to a research conducted by ITU-D Question 12-3/1 participants[75], for a successful transition, the following guidelines need to be considered:

- It is important and necessary to adapt the existing legal and institutional framework and ensure that it is fully implemented in order to promote a genuine NGN investment promotion policy.
- It is important that the national regulatory authorities take into account the risk profile of these investments when establishing tariffs in cases of mandatory access intended to promote competition.
- Structural measures should be introduced with the aim of encouraging competition and ensuring choice for consumers.

- **Quality of Service**

ITU-T recommendation E.800 defines QoS as "the collective effect of service performances, which determine the degree of satisfaction of a user of the service." QoS therefore concerns aspects of services that users experience directly. It can be contrasted with network performance, which, according to ITU-T recommendation E.800, is "the ability of a network portion to provide the functions related to communication between users." The ITU has at least 150 technical recommendations related to QoS, and several other organizations, such as ETSI and IETF, have also developed related standards[76].

Competition in a service market should positively affect the quality of the services provided, however measuring quality, establishing targets, and enforcing standards is generally more laborious than defining market incentives for operators to provide good service. Poor customer support can be a symptom of deficiencies in staff skills. High fault report rates and low proportions of successful calls generally indicate a need for improved network equipment. In a market where users and consumers can easily choose an alternate service provider, poor performance can be swiftly addressed and punished by customer churn.

- **Network Security Best Practices**

---

[74] ITU`s Bridging Standardization Gap (BSG) programme aims at increasing participation of developing countries in standardization, to ensure that developing countries experience the economic benefits of associated technological development, and to better reflect the requirements and interests of developing countries in the standards-development process. http://itu.int/go/RFQ2

[75] ITU-D Question 12-3/1, "Tariff policies, tariff models and methods of determining the costs of services on national telecommunication networks, including next-generation networks," 2014.

[76] ITU-T Recommendation E.800, "Definitions of terms related to quality of service," Sep. 2008.

Cybersecurity should be dealt with taking into consideration the global, transnational nature of cyberthreats, and in accordance with existing frameworks and coursework developed under ITU-D Question 22-1/1, as well as by other relevant expert organizations[77].

The Q22-1/1 final report[78] presents a number of best practice reports on different aspects of cybersecurity. These include (1) a guide for the establishment of a national cybersecurity management system; (2) best practices for the creation of public-private partnerships in support of cybersecurity goals and objectives; (3) building a national computer security incident management capability; (4) managing a national CIRT with critical success factors; and (5) best practices for Internet Service Provider (ISP) network protection.

- **National Broadband Plans**

A clear statement of policy objectives and/or targets can boost understanding and facilitate the national roll-out of broadband. This statement may often (but not always) take the form of a National Broadband Plan[79]. The report on the State of Broadband 2014, by the Broadband Commission[80], estimated that 140 countries have developed a national plan, strategy, project or polity to promote broadband, while a further 13 countries were planning to indroduce such measure in the near future (see Figure 3-7-2). Also, according to the same report, the number of National Broadband Plans has grown strongly since 2009, partly driven by the financial crisis, which spurred many Governments to respond with stimulus funding for broadband[81].

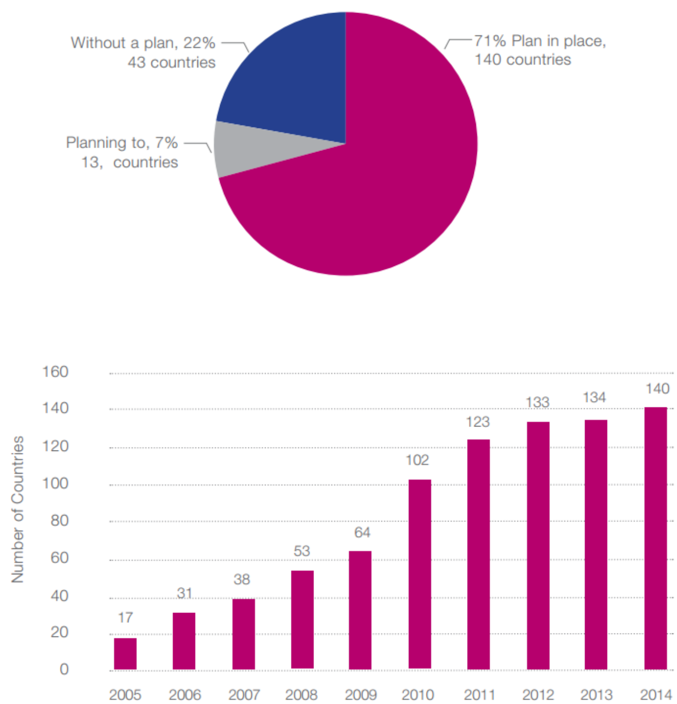



Figure 3-7-2 – National Broadband Plans

77 WTDC14, Dubai Action Plan, Objective 3.

78 Q22-1/1 final report, 2014, http://itu.int/go/F2EP

79 See GSR 2011 Discussion Paper on "Setting National Broadband Policies, Strategies and Plans", available at: http://itu.int/go/CGKE

80 Report available at http://www.broadbandcommission.org/Documents/reports/bb-annualreport2014.pdf

81 ITU "Confronting the Crisis: ICT Stimulus Plans for Economic Growth", 2009, available at: http://itu.int/go/51BT

- **Other issues on ICT policy and regulation**

The wide range and complexity of themes related with the ICT market cannot be covered in this publication. Besides the ones previously mentioned, other topics should be considered when defining ICT policies and regulations, such as: converged licencing frameworks, net neutrality, international mobile roaming, spectrum policy, cloud privacy and data protection, enforcement, intellectual property rights, IPv4 to IPv6 migration, switching from analogue to digital broadcasting, and so on.

To assist in this task ITU issues annually the Trends in Telecommunication Reform[82] publication that focuses on the latest ICT regulatory developments. This report offers insightful guidance to assist policy-makers and regulators in understanding the transnational aspects of ICT regulation in the global networked society based on the latest ITU data, research and analysis, this chapter provides an overview of the latest key market and regulatory trends that have an impact on ICT regulation.

[82] See: http://www.itu.int/pub/D-REG-TTR

## 3.9 Internet of Things

### 3.9.1. Background

The Internet of Things (IoT) is one of the hottest and one of the most divisive topics in Information and Communication Technology (ICT) today. There are many different views on the IoT, from those who judge it an ambitious concept to others who purport a kind of infrastructure. As the authors of [1] point out, this variety of viewpoints (and resulting definitions) stems from the locution itself, mixing the notion of 'Internet' – which itself can cover many different realities, from networking aspects up to a collection of socially-meaningful data and services - and the notion of 'things' – which is even more subject to interpretation, although in the IoT context it usually refers to network-able things, i.e., connected physical objects or virtual things that have a cyber-existence (a piece of content, a service, the representation of a physical object). The result is that a first splitting of viewpoints emerges, based on whether the considered actor has an Internet-oriented (i.e., focused on the communication infrastructure and mechanisms, typically resulting in the Machine-to-Machine (M2M) field) or an Object-oriented view (i.e., focused on the possibilities offered by having real-world objects reflected in the network or augmented with Information Technology (IT) services as is the case with Radio Frequency Identification (RFID) or smart objects). Another major resulting dimension, which pertains more to computer science, is the notion of complex distributed systems. As more and more heterogeneous objects get connected to an Internet of Things, novel means to manage, describe, discover, and use these connected resources and the data they produce become necessary. A number of initiatives borrowing from the fields of autonomous or intelligent systems and semantic technologies, etc. go in this direction. Figure 3-9-1 gives an idea of the variety of topics brought by these three viewpoints that make up the Internet of Things landscape. It is also important to note that this diversity of actors and viewpoints results in an equally important diversity of application fields (examples are given in Section 3.9.3). With so many diverging opinions, there have been many attempts to define the IoT so that it can move forward with a common understanding in a global perspective.

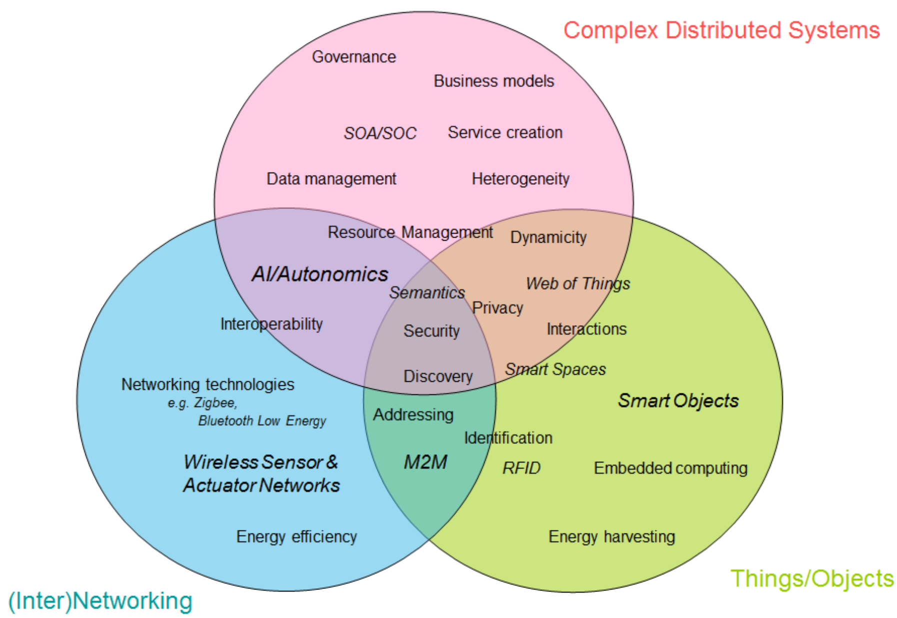



Figure 3-9-1 – The three viewpoints of the Internet of Things and their associated concepts and topics (Freely adapted from [1])

After considering the existing definitions put forth by different organizations, the ITU-T has defined the IoT as follows: "The IoT can be perceived in a broad perspective as a vision with technological and societal implications. The IoT can be viewed as a global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on both existing and evolving interoperable ICTs. Through the exploitation of identification, data capture, processing and communication capabilities, the IoT makes full use of things to offer services to all kinds of applications, whilst maintaining the required privacy" [2].

As a result of the IoT vision, many different kinds of devices connect to the network and take part in the exchange of communication. End points of this communication may be humans, or objects such as devices/machines. As a result, two distinct modes of communications are commonly described for the IoT [3, 4, 5, 6]:

- Human-to-Object (Thing) Communication: humans communicate with a device in order to get specific information (e.g., IPTV content, file transfer) including remote access to objects by humans.
- Object-to-Object (Thing-to-Thing) Communication: an object delivers information (e.g., sensor-related information) to another object with or without the involvement of humans. As objects include physical devices and products as well as logical contents and resources, M2M communication is a subset of object-to-object communication.

In the IoT, things are objects of the physical world (physical things) or of the information world (virtual things), which are capable of being identified and integrated into information and communication networks. All of these things have their associated information, which can be static and dynamic [2].

- Physical things exist in the physical world and are capable of being sensed and/or actuated upon and/or connected. Examples of physical things include sensors of surrounding environments, industrial robots, goods, and electrical equipment.
- Virtual things exist in the information world and are capable of being stored, processed and accessed. Examples of virtual things include multimedia contents, application software and service representations of physical things (e.g. avatars or Virtual Objects [7]).

Objects that contain sensors can interconnect with one another and can be monitored by distant servers or people. Many everyday objects already incorporate embedded microcontrollers and will increasingly include (often wireless) networking interfaces. Typical microcontrollers incorporate a microcomputer, storage, software, and interfaces for sensors and actuators that can reside onboard everyday objects. With the addition of a network interface, people and machines can monitor and control such objects from a distance, via the Internet. Software that resides in servers and/or in Internet-connected objects can initiate a sequence of events, with or without human intervention. The combination of embedded microcontrollers, sensors, actuators, network interfaces, and the greater Internet makes it possible for the Internet to evolve from a network of interconnected computers to a network of interconnected objects. Accordingly, the things in the IoT influence each other depending on their functional capabilities (e.g., computational processing power, network connectivity, available power, etc.) as well as on their context and situations (e.g., time, space) and will be actively involved in different processes [8]. Based on these concepts, the fundamental characteristics of the IoT are identified as follows [2]:

- Interconnectivity: Any type of thing will have the potential to be inter-connected with the communication infrastructure.
- Things-related services: The IoT is capable of providing thing-related services within the constraints of things, such as privacy protection and semantic consistency between physical things and their associated virtual things. In order to provide thing-related services within the constraints of things, the technologies in both the physical world and the world of information and communications will change.
- Heterogeneity: IoT devices are heterogeneous, ranging from tiny sensors and actuators to mobile devices and large computers, and based on different hardware platforms and networks. They can interact with other devices or service platforms through various networks.
- Dynamic changes: The state of devices changes dynamically, e.g., sleeping and waking, connected/disconnected, etc. as does their context, including location and speed. Moreover, the number of devices can change dynamically.
- Enormous scale: By 2020, there will be 50 billion things that will need to be managed and to communicate with each other [9, 10]. Even more critical will be the management of the data generated and its interpretation for application purposes. This aspect relates to the semantics of data, as well as its efficient handling.

The following sub-section introduces technology trends for beyond M2M – visions and requirements for the IoT. The state of the art and examples of the IoT are then introduced. Next, architectural models for the IoT are presented. The relevant activities for standardization are summarized in the last sub-section.

### 3.9.2. Beyond M2M

- **Towards an Internet/Web of Things and People post-M2M**

M2M is about enabling the flow of data between machines and machines, and ultimately machines and people. M2M communications involve the automated transfer of information and commands between two machines with no human intervention at either end of the system [11]. There are many different choices to make, such as how each machine is connected, what type of communication is carried out, and how the data is used. However, there are four basic stages that are common to virtually every M2M application [12]:

- Collection of data from a machine;
- Transmission of selected data through a communication network;
- Assessment of the data via integration; and
- Response to the available information depending on the circumstances.

While M2M is a specific capability that enables machines to connect and then to interact over a network, the IoT is so much more than M2M, and its potential has only just begun to be explored. The IoT it is about interacting with the objects around us, even static non-intelligent objects, and augmenting such interactions with context provided by geo-location, time and other information. In this context, M2M is a subset of the IoT [13]. Through the evolution of smart objects, a smart object becomes aware of its characteristics, context, and situation (Figure 3-9-2). These smart objects communicate with each other and with various types of mobile media and devices based on standard communication protocols. Recently, we have seen the substantial increase in the production of smart objects in everyday life thanks to the advances in embedded IT. Consumers are quickly learning how to access them, mainly through communication technologies such as Near Field Communication (NFC), accessible through smart phone applications.

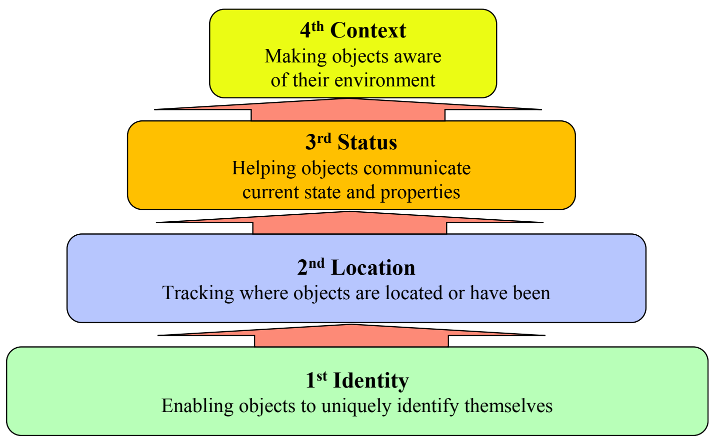



Figure 3-9-2 – The evolution of smart objects (source: [14])

Regardless of the number of low-power network protocols developed recently to facilitate these connections, embedded devices are still located in isolated islands at the application layer: developing applications using them is a challenging task that requires expert knowledge of each ecosystem. As a consequence, integrating smart objects into applications to support a smart connected world remains a difficult task. Meanwhile, the Internet with Web on top shows how open standards can be used to build millions of flexible systems over heterogeneous hardware and software platforms and still preserve efficiency and scalability. Websites no longer offer only pages, but Application Programming Interfaces (APIs) that can be used by other Web resources to create new, ad-hoc and composite applications running in the computing cloud and accessible by desktops or mobile computers. The Web of Things (WoT) [7, 15] is a way of realizing the IoT wherein everyday devices and objects are connected by fully integrating them to the Web. Web standards are used to access the capability of the devices, which makes it possible for users to interact with the devices using Web interfaces. The WoT can provide capabilities such as device reusability, portability across several heterogeneous networks, and accessibility based on the Web and with Web standards [16, 17].

Thanks to the loose-coupling, simplicity and scalability of RESTful architectures, and the wide availability of Hypertext Transfer Protocol (HTTP) libraries and clients, RESTful architectures are becoming one of the most ubiquitous and lightweight integration platforms. Using Web standards to interact with smart things thus appears to be increasingly adequate. Although HTTP introduces a communication overhead and increases the average latency, it is sufficient for many pervasive scenarios where such longer delays do not affect user experience [18, 19].

Recently, a new approach for a human interaction model for the IoT, the so-called 'Social WoT' [20, 21], has been introduced as an interaction paradigm for connecting people to the IoT. While the IoT has focused mainly on establishing connectivity in a variety of challenging and constrained networking environments, the social WoT enables interactions among people to be translated into representations in the real physical world in a way that provides some of the same ambient awareness that the social network services provide online. Therefore, it allows people to connect, use, share and compose physical and virtual things in order to create personalized and pervasive applications.

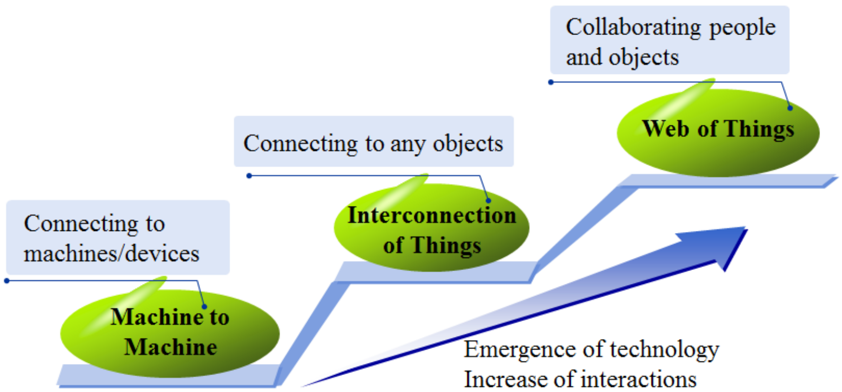



Figure 3-9-3 – Evolution of the Internet of Things technology

Figure 3-9-3 shows the technical evolution from M2M to WoT. When we consider various devices, including tiny sensors for M2M, providing connectivity is the fundamental challenge for the communication technology. From the interconnecting of things, to link to any object in the real world will be as critical as the extension of end points. In addition, Web-enabled objects (i.e., WoT) will support the easy creation of applications and sharing of data from objects and people.

A recent white paper [22] points out that a 'pluridisciplinary' approach to develop the requisite new technologies, concepts, and models is needed. This would include Integrated Circuit development, energy management, communications systems and principles, embedded systems, and packaging data acquisition and processing. Among the key challenges for the IoT, the following three points should demand the most attention:

- Integration of smart, autonomous interconnected objects such as sensors, actuators and processors working under severely constrained energy and physical environments;
- Coping with the potentially billions of objects [9] that can be interconnected over secure, flexible networks providing secure and ubiquitous service provisioning; and
- Accomplishing the fusion of the data obtained by sensors, the network and service management, distributed data treatment, and ambient intelligence.

- **Vision and impact**

The vision of the IoT suggests that there would be a "world-wide network of interconnected objects uniquely addressable, based on standard communication" [23]. Everything from individuals, groups, communities, objects, products, data, services, and processes will potentially be connected by the IoT. Connectivity will become, in the IoT, a kind of commodity. In addition, there will be the need to create the best situation-aware development environment for stimulating the creation of services and appropriate intelligent middleware to understand and interpret the information, to ensure protection from fraud and malicious attack and to guarantee privacy [9].

With this vision, and making use of intelligence in the supporting network infrastructure, things will be able to autonomously manage their transportation, implement fully automated processes, and thereby optimize logistics. They may be able to harvest the energy they need. They will automatically configure themselves when exposed to a new environment; exhibit an 'intelligent/cognitive' behavior when faced with other things, and deal seamlessly with unforeseen circumstances. Ultimately, they could even manage their own disassembly and recycling at the end of their lifecycle, helping to preserve the environment and freeing humans from exposure to dangerous components.

The IoT infrastructure allows combinations of smart objects, sensor network technologies, and human beings, using different but interoperable communication protocols, capable of realizing a dynamic multimodal/heterogeneous network that can be deployed in inaccessible or remote locations and in cases of emergencies or hazardous situations. In this infrastructure, different entities or things discover and explore each other and learn to take advantage of each other's data by pooling resources, dramatically enhancing the scope and reliability of the resulting services.

The IoT can benefit from the latest developments and functionalities through the provision of new, intuitive user-centered and individually configurable, self-adapting smart products and services for the benefit of businesses and society [24].

Figure 3-9-4 summarizes the vision and impact of the IoT. One of the ultimate objectives of the IoT is to meet the challenge of seamless communications between any things (e.g., humans and objects). The IoT will have to encompass the following:

- Ubiquitous connectivity allowing for whenever, whoever, wherever, and whatever types of communications;
- A pervasive reality for effective interfaces to provide connectable real world environments; and
- Ambient intelligence allowing for innovative communications and providing increased value creation.

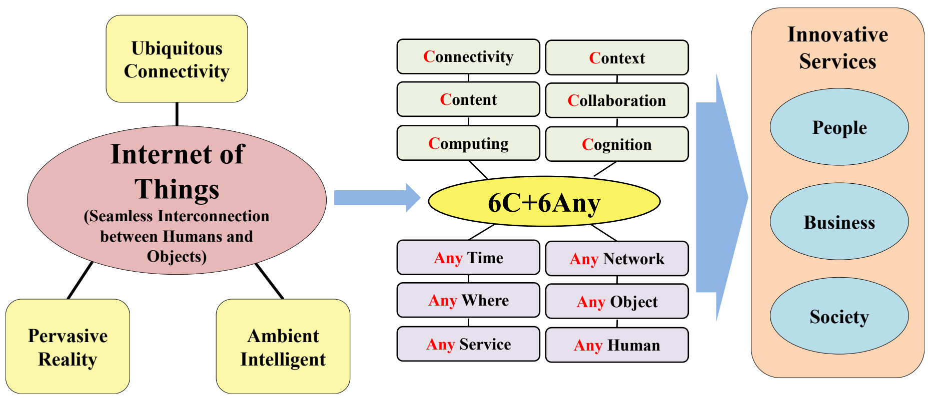



Figure 3-9-4 – The Internet of Things: vision and impact

From communications for transmitting information, evolution will effectively integrate connectivity and content with computing, context, collaboration and cognition. Therefore, the IoT will be a global network of interconnected objects, enabling the identification and discovery of objects as well as semantic data processing via 6Cs+6Anys [5, 25]. Here, the 6Cs include:

- Connectivity: connection for mobile and constrained objects;
- Content: massive data produced from objects;
- Computing: cloud computing and content storage service;
- Context: context aware design to improve performance;
- Collaboration: cooperative communications, inter-objects and service sharing;
- Cognition: mining the knowledge from massive data and providing autonomous system adjustment for improvements.

6Anys stands for Any time, Any where, Any service, Any network, Any object and Any human.

From the vision, the IoT is beginning to transform how we do business, the run the public sector and the daily life of people. The IoT will thus enable innovative services for people, business and society involving the use of technologies such as Bio Technologies (BT), Nano Technologies (NT) and Content Technologies (CT), thereby allowing the provision of services that go beyond traditional telecommunication and IT services. These innovative services, including interdisciplinary services, will require extensions in terms of networking and service capabilities as well as the availability of all sorts of objects [5, 26].

- **Requirements**

The following is a list of high-level requirements that have specific relevance for the IoT [2, 3, 27]:

- Each object will need to be connected to the network and be able to consider heterogeneous identifiers. It is necessary to support the identification of each object and provide seamless communication via the association with the network, as well as tracking of the object with no restrictions on the location.
- Interoperability must be ensured among heterogeneous and distributed systems for the provision and consumption of a variety of information and services and seamless interaction among objects.

- For small-sized objects with limited power, their capabilities as communication objects are less (sometimes much less) than those of higher-end processing and computing devices. To cope with these constrained objects, lightweight protocols that remove unnecessary loads/messages and minimize energy consumption become a necessity.
- Autonomic networking (e.g., self-management, self-configuring, self-healing, self-optimizing (learning) and self-protecting techniques and/or mechanisms) needs to be supported so that objects can adapt to different application domains, different communication environments and a wide variety of devices. To support self-configuration, context information plays a critical role in supporting context-aware networking for changing communication environments, and in supporting a semantic as the virtual representation of physical objects.
- For autonomic service provisioning, the services need to be able to be provided by the automatic capture, communication and processing of the data of things based on the rules configured by operators or customized by subscribers. Autonomic services may depend on the techniques of automatic data fusion and data mining.
- Objects can move from one place to another and may become attached to another network with a different technology. Object mobility management is required to provide seamless communication among mobile objects for location-based communications and services. This may be constrained by laws and regulations, and should comply with security requirements.
- Network size is increasing as more and more objects are connected to the network. Scalable solutions are required in order to cope with the increase of traffic and routing table sizes and the shortage of IP addresses.
- To support end-to-end connectivity, each object will need to be addressable and should therefore have a unique address. Adequate address space is a prerequisite to allow the huge number of objects expected in the IoT to be connected to the network. Alternatively, each object would be required to provide their direct connectivity via a host or gateway with a unique IP address.
- The required Quality of Service (QoS) and Quality of Experience (QoE) levels must be respected. Reliable services require on-time handling along with a verifiable level of accuracy.
- Security and privacy concerns must be managed appropriately, as the IoT connects many sophisticated objects, which may cause untold damage –even life-threatening damage – if their security is breached. The IoT needs to support privacy protection during data transmission, aggregation, storage, mining and processing.
- Self-management must be supported to ensure normal network operations. IoT applications usually work automatically without human participation, but their overall operation process should be manageable by the relevant parties.
- Middleware architectures for the IoT often follow the Service Oriented Architecture (SOA) approach. The adoption of the SOA principles is required for the decomposing of complex and monolithic systems into applications consisting of an ecosystem of simpler, well-defined components [1].

### 3.9.3. The State of the Art and Examples

- **Key technologies for the IoT**

Progress in the following technologies will contribute to the development of the IoT as its enabling building blocks [4]:

- M2M interfaces and electronic communication protocols to set the rules of engagement for two or more nodes on a network.
- Embedded computing with the computer chips (e.g., microcontrollers) that are designed to be embedded into objects other than computers.
- Wireless communication, which has the potential to play an important role in the IoT, including short-range and long-range channels as well as bidirectional and unidirectional channels.
- RFID technology, which can identify multiple objects concurrently. Some RFID tag-reader architectures support security features such as requiring a human operator to input a challenge code before decoding an ID. RFID can have varying sizes (from a few cm to hundreds of meters), power requirements, operating frequencies, amounts of rewriteable and nonvolatile storage, and software intelligence.
- Energy harvesting technologies to capture small but usable amounts of electrical energy from the environment. Current energy-harvesting research and development concentrates on advantageous temperature variations, ambient sound and vibration, and ambient radio frequency.

- Sensors that can detect changing attributes in the environment and report them to a system, along with sensor networks to exploit the benefits of sensing at more than one location. Actuators detect an incoming signal and respond by changing something in the environment.
- Location technology to assist people and machines in locating objects and to determine their physical whereabouts. For example, fixed or orbiting transmitters have known locations. They can broadcast timing signals, and receiving devices triangulate by calculating the amount of delay from each transmitter.
- Software comprises a broad domain of development. Development of the IoT will rely on many dimensions of software capabilities, including distributed execution, self-describing data structures, and much more.

- **IoT examples**

From the key characteristics of the IoT, new opportunities can be created to meet business requirements: creating new services based on real-time physical world data, gaining insights into complex processes and relationships, handling incidents, addressing environmental degradation (e.g., pollution, disaster, global warming, etc.), monitoring human activities (e.g., health, movements, etc.), improving infrastructure integrity (e.g., energy, transport, etc.), and addressing energy efficiency issues (e.g., smart energy metering in buildings, vehicles' fuel efficiency, etc.) [8].

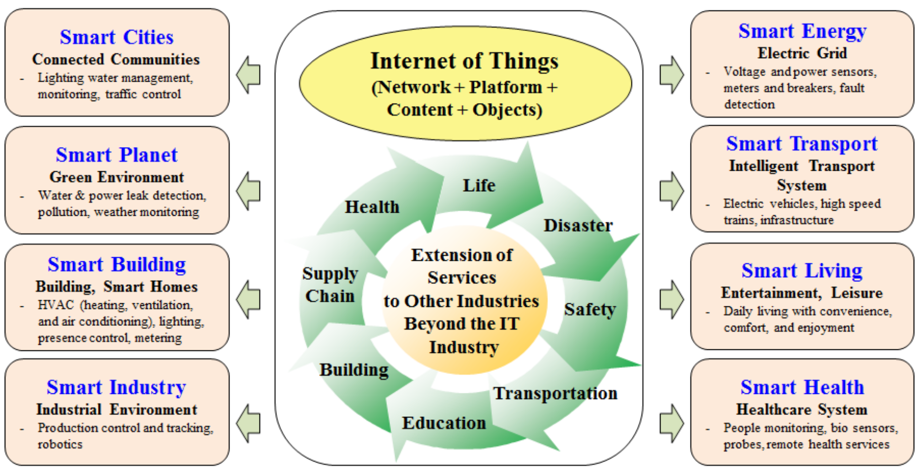


Figure 3-9-5 – Internet of Things examples (illustration inspired from [5, 28])

The IoT is disruptive and will omnipresent. Accordingly, the IoT will significantly impact all fields of our lives in the future. As shown in Figure 3-9-5, the major application fields for the IoT are the creation of smart environments/spaces and self-aware things (e.g., smart transport, cities, buildings, energy, living spaces, etc.) that will be activated to realize logistic, agriculture, food, energy, mobility, digital society and e-health applications [28, 29]. In the IoT, applications can be created through the integration and combination of technologies such as BT, NT and CT. Therefore, it is necessary to combine BT, NT, CT as well as IT in support of network, platform, content and objects for the IoT.

Communication networks have been supporting the evolution of information processing and service capabilities within IT industries. However, the capabilities of networks benefiting from ubiquitous networking will soon be impacting other industries such as medical technology, education, finance, transportation/ distribution, etc., resulting in new requirements for specific services to be incorporated into the IT field [3].

### 3.9.4. Architecture Model

- **IoT ecosystems**

The IoT sets the stage for a business ecosystem composed of a variety of business roles and players. Each business player could play at least one business role, but additional roles are possible. Some of the identified IoT business roles are shown in Figure 3-9-6 [2]. The identified business roles and their relationships do not represent all the possible relevant roles and relationships that can be found across IoT business deployments.

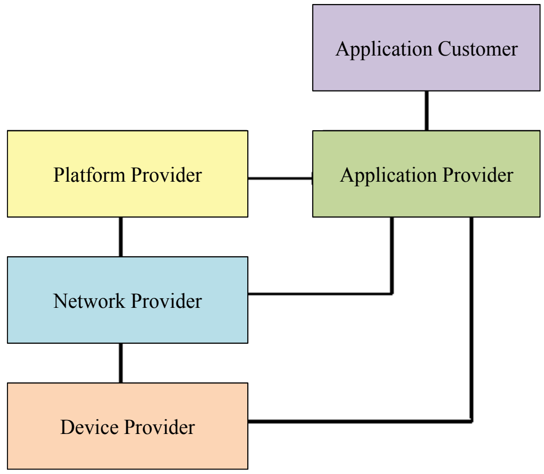


Figure 3-9-6 – An Internet of Things ecosystem (illustration from ITU-T Y.2060 [2])

- The device provider is responsible for devices, providing raw data and/or content to the network provider and the application provider according to the service logic.
- The network provider plays a central role in the IoT ecosystem. In particular, the network provider performs the following main functions:
  - Access and integration of resources provided by other providers;
  - Support and control of the IoT capabilities' infrastructure; and
  - Offering the IoT capabilities, including network capabilities and resource exposure to other providers.
- The platform provider provides integration capabilities and open interfaces. A platform serves as a foundation or base for realizing a particular functionality. Different platforms can provide different capabilities to application providers. Platform capabilities include typical integration capabilities, as well as data storage, data processing, device management etc. Support for different types of IoT applications is also possible.
- The application provider utilizes capabilities or resources supplied by the network provider, device provider and platform provider to deliver IoT applications to application customers.
- The application customer is a user of IoT application(s) provided by the application provider.

The rest of this sub-section provides details of the architectural aspects in each layer related to the IoT ecosystem. First we present the IoT reference model and functional groups, and then describe enablers and an implementation model to support the IoT.

- **IoT reference model and functional groups**

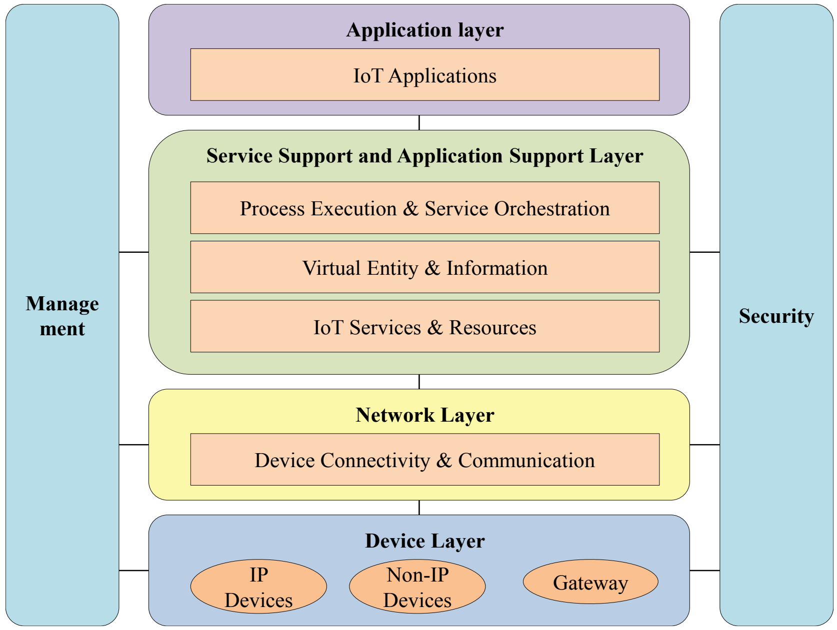



Figure 3-9-7 – Internet of Things reference model and functional groups (illustration compiled from ITU-T Y.2060 [2] and IoT-A [30])

Figure 3-9-7 shows the IoT reference model and its functional groups, which began as a reference model from ITU-T [1]. The relevant functional groups developed by the IoT-A project [30] are shown in the figure to make the key functionalities of each layer clearer.

The IoT reference model is composed of four layers (application, service support/application support, network, and device layers) as well as management and security capabilities associated with the four layers [2]. From a functional viewpoint, seven functional groups (IoT Applications, Process Execution & Service Orchestration, Virtual Entity & Information, IoT Service & Resources, Device Connectivity & Communication, Management, and Security) were identified to meet the requirements in the IoT-A [30]. The following items explain the information shown in Fig. 7 in more detail:

- The application layer contains IoT applications.
  - IoT Applications: This group describes the functionalities provided by applications that are built on top of an implementation of the IoT architecture.
- The service support and application support layer consists of the following two capabilities: 1) Generic support capabilities, which are common capabilities that can be used by different IoT applications, such as data processing and data storage; and 2) Specific support capabilities to cater to the requirements of diverse applications. These may consist of various detailed capability groupings assembled to provide different support functions to different IoT applications.
  - Process execution & service orchestration: This functionality group organizes and exposes IoT resources so that they become available to external entities and services. Through this set of functionalities, and the APIs that expose them, IoT services become available to external entities and can be composed by them.
  - Virtual entity & information: This group maintains and organizes information related to physical entities, enabling the search for services that expose resources associated with physical entities. It also enables the search for services based on the physical entity they are associated with. When queried about a particular physical entity, this functionality group will return the addresses of the services related to that particular physical entity.
  - IoT service & resource: When queried about a specific service, this group will return its description, providing links to the exposed resources. This group also provides the functionalities required by services for processing information and for notifying application software and services about events related to resources and corresponding physical entities.

- The network layer consists of the following two types of capabilities: Networking capabilities that provide the relevant control functions related to network and device connectivity; and transport capabilities focused on providing connectivity for the transport of IoT service/application specific data information, as well as the transport of IoT-related control and management information.
  - Device connectivity & communication: This functional block provides the set of methods and primitives required for device connectivity and communication (the first referring to the possibility for a device to be part of a network, the second to the possibility for that device to be a source of or destination for messages). This group also contains methods for content-based routing.
- The device layer can be logically categorized into three kinds of capabilities: IP device capabilities, Non-IP device capabilities and gateway capabilities. Each device in the device layer needs to support one or more of the following capabilities:
  - Direct communication with the network layer for IP devices: devices that can gather and upload information directly (i.e., without using gateway capabilities) to the network layer and directly receive information (e.g., commands) from the network layer;
  - Indirect communication with the network layer for non-IP devices: devices that can gather and upload information to the network layer indirectly, i.e., through gateway capabilities; and
  - Gateway capabilities: gateway capabilities include but are not limited to:
    - ✓ Support for multiple interfaces: Support for devices in the direct layer to be connected to the network layer via various types of wired or wireless technologies, such as controller area network bus, ZigBee, Bluetooth, Wi-Fi, etc. Within the network layer, the gateway capabilities can communicate through various technologies, such as Public Switched Telephone Network (PSTN), Second Generation/Third Generation (2G/3G), Long Term Evolution (LTE), Ethernet, and Digital Subscriber Line (DSL).; and
    - ✓ Protocol conversion: There are two situations where IoT gateway capabilities are needed. One is when communications at the device layer use different device-layer protocols, e.g., ZigBee technology protocols and Bluetooth technology protocols. The other situation is when inter-layer communications use different protocols, e.g., ZigBee technology protocol at the device layer and a 3G technology protocol at the network layer.
- Management: To manage computational resources efficiently, management should be administered by a group of functionalities.
  - Device management, such as remote device activation and de-activation, diagnostics, firmware and/or software updating, sensor node working status management;
  - Sensor network topology management; and
  - Traffic and congestion management, such as the detection of network overflow conditions and the implementation of resource reservation for time-critical and/or life-critical data flows.
- Security: Security functions must be applied consistently by the different groups of functionalities. Specifically, access-control policies should be applied consistently to prevent unauthorized applications from obtaining access to sensitive resources.
  - At the application layer, these include authorization, authentication, application data confidentiality and integrity protection, privacy protection, security audit and anti-virus programs and policies;
  - At the network layer, security needs motivate the use of authorization, authentication, use data and signaling data confidentiality programs, signaling integrity protection policies, etc.; and
  - At the device layer, secure procedures include authentication, authorization, device integrity validation, access control, data confidentiality and integrity protection programs.

In the next section, more specific enabling functionalities are shown to identify key capabilities from a generic reference model and standard functional groups.

- **Generic enablers and implementation model to support the IoT**

The relevant Generic Enablers (GEs) for IoT service enablement were specified by FI-WARE [31], making it possible for objects to become citizens of the Internet – available, searchable, accessible, and usable – so that future Internet services can create value from real-world interaction, enabled by the ubiquity of heterogeneous and resource-constrained devices.

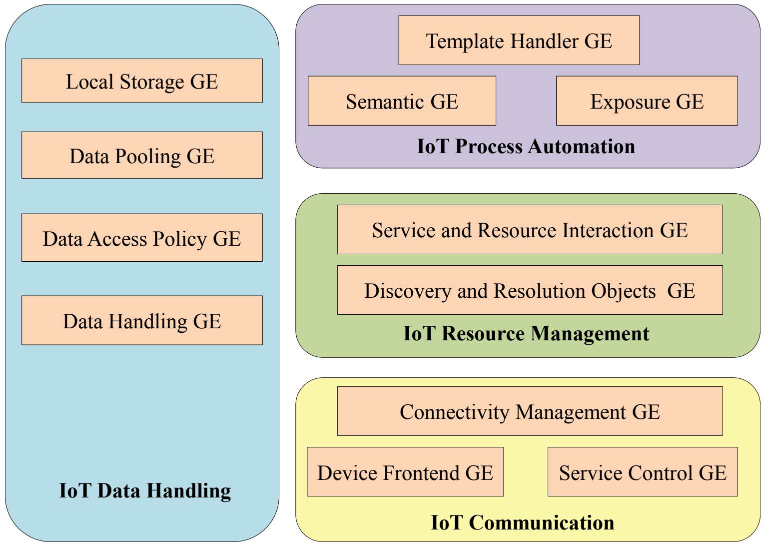


Figure 3-9-8 – Internet of Things generic enablers (GEs) (illustration from FI-WARE [31])

Management functionalities are provided for the devices and IoT domain-specific support is provided for the applications. As shown in Figure 3-9-8, there are four groups of GEs for the IoT service enablement to be adopted and integrated:

- IoT Communications provide common and generic access to every kind of thing, regardless of any technological constraint on communications, typically having to integrate several protocols and manage the discontinuity of connectivity for nomadic devices. The GEs for IoT communications allow application providers to gain homogeneous access to dedicated things and devices and to be able to manage QoS in communication with those devices.
- IoT Resource Management proposes unified service and operational support management functions, enabling the different IoT applications and end users to discover, utilize and activate small or large groups of IoT resources and manage their properties. In doing so, the IoT service enablement focuses on global identification and information model schemes for IoT resources, providing a resolution infrastructure to link them with relevant things and developing a common remote management tool for configuring, operating and maintaining IoT resources on a large scale and with minimum human intervention.
- IoT Data Handling is essential for application and data service providers to collect large amounts of IoT-related data, produced by a huge number of IoT resources almost in real-time. The GEs for IoT data handling are supported by security- and privacy-regulated policies in their collecting and forwarding of data to application/services.
- IoT Process Automation provides application/service providers with generic automation capabilities, enabling them to use subscription and rules templates that ease the programming of automatic processes involving IoT resources. They allow high-level conditions to be set up, which may in turn trigger new actions in a self-propagating process.

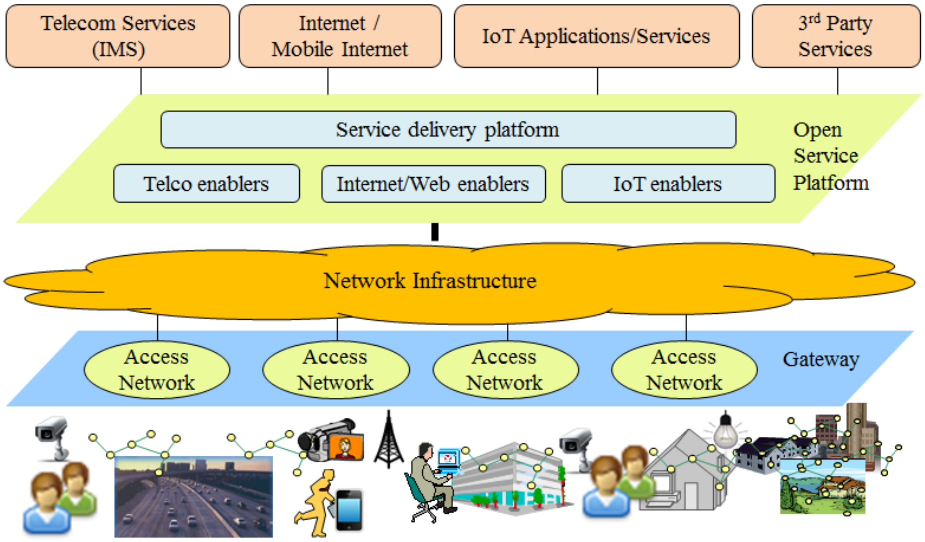


Figure 3-9-9 – An implementation model for the Internet of Things

As shown in Figure 3-9-9, from the telecom operators' perspective, they have a network infrastructure and service platform for providing telecom services using IP Multimedia Subsystem (IMS) and (mobile) Internet services thorough telecom enablers and Internet/Web enablers, which includes related capabilities for location, presence, calls, messaging, multimedia and so on. A service delivery platform for converged services and IoT enablers can support various IoT applications and services as well as 3rd party services through an open service platform, as shown in Fig. 8. A unified service delivery platform is needed to integrate resources from different networks and support multiple applications. That unified platform thus allows telecom operators to have a major role in the overall ecosystem through service creation, service execution and service delivery management. A telecom operator also needs to support access networks with various wired/wireless interfaces via gateways, according to the local environment.

This sub-section presented an architectural model based on results from standards and related projects. The IoT functional model promotes a common understanding of the IoT. In particular, the analysis of an IoT reference model and its functional groups provides a favorable positioning of key capabilities. The IoT GEs make a large number of things and associated resources to become available, searchable, accessible and usable for the enabling IoT services. Finally, this section has provided an implementation model for the IoT in the telecom operator perspective.

### 3.9.5. Standardization for the IoT

The growth of the IoT industry has led to the need for interoperability between IoT solutions. Towards this direction, all major standardization bodies have established working groups dedicated to IoT technology. Most Standards Developing Organizations (SDOs) have only recently been formed and the overall specifications are therefore still under development. Few specifications have been published; these mainly address the overall system requirements and architecture and do not delve into the specifics of detailed solutions. The recent activities of SDOs related to the IoT are presented here to identify the gaps and to focus the search for new items for future standardization [32, 33].

- **Third-Generation Partnership Project (3GPP)**

There is a significant amount of on-going standards work focused on M2M communications. The initial M2M standardization effort in 3GPP was started by the Service and System Aspect Working Group 1 (SA1 WG), which defined the service requirements for Machine Type Communications (MTCs). During the study of MTCs in 3GPP, the SA1 WG identified two scenarios:

- MTC devices communicating with one or more MTC servers. The network operator provides network connectivity to MTC servers. This applies to MTC servers controlled by a network operator as well as to MTC servers not controlled by a network operator.
- MTC devices communicating with each other. Due to the complexity and uncertainty of an actual deployment, this scenario is not considered in the current version (Release 10), but may be considered in future releases.

Since the domain of M2M communications is fairly wide, not every system optimization scheme is suitable for every MTC application. Therefore, a list of MTC features has been developed to provide a structural approach to help investigate the different system optimization possibilities. Some examples of these MTC features are low mobility, location-specific triggers, infrequent transmission, and group-based MTC features.

- **Third-Generation Partnership Project 2 (3GPP2)**

Three major activities in 3GPP2 are related to the M2M field: developing an M2M study report, investigating the impact of existing numbering schemes used as device and subscription identities for M2M devices over a Code Division Multiple Access (CDMA) network, and working on network enhancements to accommodate future M2M devices.

The study also reports that architectural enhancements, such as various M2M communication models, need to be considered for efficient network operation. Moreover, the architecture might need a communication adaptation protocol and a new terminal class for M2M devices so that the network can distinguish M2M devices from traditional wireless devices. Potential M2M-related enhancements to the 3GPP2 radio network are also identified.

Another M2M activity at the 3GPP2 Steering Committee (SC) level is to investigate the impact on the current addressing and numbering schemes due to the presence of a large number of M2M devices in the cdma2000 network.

- **European Telecommunications Standards Institute (ETSI)**

The ETSI has published the first release of its M2M service standards, providing a standardized platform to manage the complexity of multiple M2M services and technologies.

M2M communication services are already showing strong revenue growth with the number of deployments steadily increasing. Large-scale managed M2M services will become a feature of this industry, but today the technology landscape is fragmented, which discourages investment.

Leading industry players participating in ETSI's Technical Committee (TC) for M2M communications (i.e., TC M2M) have now developed a set of standards which provides a complete horizontal service layer for M2M communications. The ETSI TC M2M standardization work mainly focuses on the service middleware layer, not the underlying access and network transmission technologies. M2M services will be implemented on top of three entities: the M2M service platform, M2M gateways, and M2M terminals. To support a wide range of M2M applications, the ETSI TC M2M is defining a set of standardized service capabilities (in all layers) that provide functions that are shared by the different M2M applications. These service capabilities can use core network functionalities through a set of exposed interfaces and can interface to one or more core networks. This set of service capabilities can be implemented in an M2M platform located in the network domain, in an M2M device (terminal), or in an M2M gateway [34].

The ETSI M2M Release 1 standards enable the integration of different M2M technology choices into one managed platform. ETSI M2M Release 1 is built upon proven and mature standards from the ETSI and other bodies such as the IETF, 3GPP, the Open Mobile Alliance (OMA) and the Broadband Forum. The business benefits are clear: reduced complexity of M2M deployments, reduced deployment time for new M2M services, and ultimately reduced costs for operation and investment, etc. The ETSI M2M standards specify architectural components including M2M devices, gateways with associated interfaces, applications and access technologies, as well as the M2M Service Capabilities Layer. They also offer security, traffic scheduling, device discovery and lifecycle management features. The ETSI M2M Release 1 standards are published as a set of three specifications available for download from the ETSI website [35]:

- Requirements in ETSI TS 102 689;
- Functional architecture in ETSI TS 102 690; and
- Interface descriptions in ETSI TS 102 921.

The publication of the ETSI M2M Release 1 standards marks a new milestone for the M2M industry. They unlock the potential for wide-scale deployment of M2M services and technologies, and encourage investment in new applications, which one day will bring about a true IoT.

- **International Telecommunication Union (ITU)**

ITU-T, Internet of Things Global Standards Initiative (IoT-GSI)

The IoT-GSI [36] promotes a unified approach in ITU-T for the development of technical standards (Recommendations) enabling the IoT on a global scale. The ITU-T Recommendations were developed under the IoT-GSI by the various ITU-T Questions groups, in collaboration with other SDOs, and will enable worldwide service providers to offer the wide range of services expected by this technology. IoT-GSI also aims to act as an umbrella for IoT standards' development worldwide.

The IoT-GSI aims to accomplish the following objectives through meetings and related activities involving groupings of rapporteur groups working on the IoT:

- Develop a definition of the 'IoT';
- Provide a common working platform by collocating meetings of IoT-related rapporteur groups; and
- Develop the detailed standards necessary for IoT deployment, taking into account the work accomplished in other SDOs.

ITU-T, Focus Group on Machine-to-Machine Service Layer (FG M2M)

The ITU's new Focus Group on the M2M (i.e. FG M2M) [37] was established in April 2012.

Considering the wide range of M2M's possible applications – enabling services across vertical markets including healthcare, logistics, transport, utilities and countless others – while these predictions may hold true, they certainly cannot be realized without the interoperability enabled by global ICT standards. A common M2M service layer, agreed to at the international level by stakeholders in the M2M and relevant vertical markets, will provide a cost-efficient platform that could easily be deployed across hardware and software platforms, in a multi-vendor environment, and across industry sectors.

The FG M2M has been identifying a minimum set of requirements common to vertical markets, and thereby creating the knowledge base needed to begin the development of open, international ITU standards. In analyzing the requirements of vertical markets, the group is initially focusing on the healthcare market by investigating APIs and protocols supporting e-health applications and services.

ITU-T, Study Group 20

Study Group 20 is working to address the standardization requirements of Internet of Things (IoT) technologies, with an initial focus on IoT applications in smart cities and communities (SC&C).

SG20 develops international standards to enable the coordinated development of IoT technologies, including machine-to-machine communications and ubiquitous sensor networks. A central part of this study is the standardization of end-to-end architectures for IoT, and mechanisms for the interoperability of IoT applications and datasets employed by various vertically oriented industry sectors.

The deployment of IoT technologies is expected to connect an estimated 50 billion devices to the network by year 2020, impacting nearly every aspect of our daily lives. IoT is contributing to the convergence of industry sectors, and SG20 provides the specialized IoT standardization platform necessary for this convergence to rest on a cohesive set of international standards.

An important aspect of SG20's work is the development of standards that leverage IoT technologies to address urban-development challenges.

IoT is a key enabler of the Information Society and offers an opportunity to transform city infrastructure, benefiting from the efficiencies of intelligent buildings and transportation systems, and smart energy and water networks. SG20 will assist government and industry in capitalizing on this opportunity, providing a unique platform to influence the development of international IoT standards and their application as part of urban-development master plans.

So far, the following IoT related recommendations have been developed in the ITU-T:

| Topic | Document title |
|---|---|
| General | • Y.4000: Overview of the Internet of things<br>• Y.4001: Machine socialization: Overview and reference model<br>• Y.4002: Machine socialization: Relation management models and descriptions |
| Definitions and terminologies | • Y.4050: Terms and definitions for the Internet of things |

| | |
|---|---|
| Requirements and use cases | • Y.4100: Common requirements of the Internet of things<br>• Y.4101: Common requirements and capabilities of a gateway for Internet of things applications<br>• Y.4102: Requirements for Internet of things devices and operation of Internet of things applications during disasters<br>• Y.4103: Common requirements for Internet of things (IoT) applications<br>• Y.4104: Service description and requirements for ubiquitous sensor network middleware<br>• Y.4105: Requirements for support of ubiquitous sensor network (USN) applications and services in the NGN environment<br>• Y.4106: Requirements and functional model for a ubiquitous network robot platform that supports ubiquitous sensor network applications and services<br>• Y.4107: Requirements for water quality assessment services using ubiquitous sensor networks (USNs)<br>• Y.4108: NGN service requirements and capabilities for network aspects of applications and services using tag-based identification<br>• Y.4109: Requirements for the support of machine-oriented communication applications in the next generation network environment<br>• Y.4110: Service and capability requirements for e-health monitoring services<br>• Y.4111: Semantics based requirements and framework of the Internet of things<br>• Y.4112: Requirements of the plug and play capability of the Internet of things<br>• Y.4113: Requirements of the network for the Internet of things |
| Infrastructure, connectivity and networks | • Y.4250: Sensor control networks and related applications in a next generation network environment<br>• Y.4251: Capabilities of ubiquitous sensor networks for supporting the requirements of smart metering services<br>• Y.4252: Energy saving using smart objects in home networks |
| Frameworks, architectures and protocols | • Y.4400: Framework of the web of things<br>• Y.4401: Functional framework and capabilities of the Internet of things<br>• Y.4402: Requirements and functional architecture for the open ubiquitous sensor network service platform<br>• Y.4403: Functional requirements and architecture of the next generation network for support of ubiquitous sensor network applications and services<br>• Y.4404: Framework of object-to-object communication for ubiquitous networking in next generation networks<br>• Y.4405: Architecture of a system for multimedia information access triggered by tag-based identification<br>• Y.4406: Functional requirements and architecture of the NGN for applications and services using tag-based identification<br>• Y.4407: Framework of networked vehicle services and applications using NGN<br>• Y.4408: Capability framework for e-health monitoring services<br>• Y.4409: Requirements and architecture of the home energy management system and home network services<br>• Y.4410: Architectural overview of next generation home networks<br>• Y.4411: Overview of application programming interfaces and protocols for the machine-to-machine service layer<br>• Y.4412: Requirements and reference architecture for audience-selectable media service framework in the IoT environment<br>• Y.4413: Requirements and reference architecture of the machine-to-machine service layer<br>• Y.4414: Web of things service architecture<br>• Y.4450: Overview of Smart Farming based on networks<br>• Y.4451: Framework of constrained device networking in the IoT environments<br>• Y.4452: Functional framework of web of objects<br>• Y.4453: Adaptive software framework for Internet of things devices |
| Services, applications, | • Y.4551: Service description and requirements for multimedia information access triggered by tag-based identification |

| | |
|---|---|
| computation and data processing | • Y.4552: Application support models of the Internet of things<br>• Y.4553: Requirements of smartphone as sink node for IoT applications and services |
| Management, control and performance | • Y.4700: Deployment guidelines for ubiquitous sensor network applications and services for mitigating climate change<br>• Y.4701: SNMP-based sensor network management framework<br>• Y.4702: Common requirements and capabilities of device management in the Internet of things |
| Identification and security | • Y.4800: Requirements and functional architecture of an automatic location identification system for ubiquitous sensor network applications and services<br>• Y.4801: Requirements and common characteristics of the IoT identifier for the IoT service<br>• Y.4802: Multimedia information access triggered by tag-based identification - Registration procedures for identifiers<br>• Y.4803: Information technology – Automatic identification and data capture technique - Identifier resolution protocol for multimedia information access triggered by tag-based identification<br>• Y.4804: Multimedia information access triggered by tag-based identification - Identification scheme |
| Evaluation and assessment | • Y.4900: Overview of key performance indicators in smart sustainable cities<br>• Y.4901: Key performance indicators related to the use of information and communication technology in smart sustainable cities<br>• Y.4902: Key performance indicators related to the sustainability impacts of information and communication technology in smart sustainable cities<br>• Y.4903: Key performance indicators for smart sustainable cities to assess the achievement of sustainable development goals |

ITU-R

ITU-R's "Wide Area Sensor Networks" essentially deals with M2M communications. ITU-R Working Party 5A is focused on "Mobile wireless access systems providing telecommunications for a large number of ubiquitous sensors and/or actuators scattered over wide areas as well as machine communications in the land mobile service", under Study Group 5 Question ITU-R 250-1/5.

- **Open Mobile Alliance (OMA)**

The scope of the OMA [38] is to develop mobile service enabler specifications to support the creation of interoperable end-to-end mobile services. Towards this direction, the OMA promotes service enabler architectures and open enabler interfaces that are independent of the underlying wireless networks and platforms. OMA's data service enablers are intended to work across multiple devices, service providers, operators, networks, and geographies.

As there are several OMA standards that map into the ETSI M2M framework, a link has been established between the two standardization bodies in order to provide associations between ETSI M2M Service Capabilities and OMA Supporting Enablers [39]. Specifically, the expertise of OMA in abstract, protocol-independent API creation, as well as the creation of API protocol bindings (i.e., REST, SOAP) and especially the expertise of OMA in RESTful APIs is expected to complement the standardization activities of ETSI in the field of M2M communications. Additionally, OMA has identified areas where further standardization will enhance support for generic M2M implementations, i.e.:

- Device management;
- Network APIs addressing M2M service capabilities;
- Location services for mobile M2M applications; and
- The messaging of sleeping M2M devices.

The overall aim of the collaboration between ETSI and OMA is twofold. On the one hand, it must be ensured that the APIs defined by OMA to describe service capabilities map into the ETSI M2M framework. On the other hand, there must be a mapping of OMA service enablers to the ETSI M2M framework.

- **Internet Engineering Task Force (IETF)**

IETF Working Groups (WGs) [40] are created to address specific problems or to produce one or more specific documents aimed at speeding up the standardization process. The duration of these groups depends solely on the achievement of their objectives, and they manage almost all of the work through mailing lists. Each WG has a charter, which specifies the scope of the work to be carried out and lists how the objectives will be achieved. Currently, there are three active working groups dealing with protocols for the IoT, covering routing, IP-based addressing and application domains:

- 6LowPAN(IPv6 over Low power WPAN): An international open standard for IP enablement of the smallest devices, such as sensors and controllers, by enabling IEEE 802.15.4 and IP together;
- ROLL(Routing Over Low power and Lossy networks): Routing over low power and lossy networks via ZigBee and Bluetooth; and
- CORE (Constrained RESTful Environments): A framework for resource-oriented applications designed to run on constrained IP networks.

In addition, a WG for implementation guidance in lightweight TCP/IP protocol suites for constrained devices has been set up:

- LWIG (Light-Weight Implementation Guidance): This WG focuses on helping the implementers of the smallest devices. The goal is to be able to build minimal yet interoperable IP-capable devices for the most constrained environments.

- **Open Geospatial Consortium (OGC)**

OGC members work to specify interoperability interfaces and metadata encodings that enable real time integration of heterogeneous sensor Webs into the information infrastructure. Developers will use these specifications in creating applications, platforms, and products involving Web-connected devices such as flood gauges, air pollution monitors, stress gauges on bridges, mobile heart monitors, Webcams, and robots, as well as space and airborne earth-imaging devices. OGC members have developed and tested the following candidate specifications [41, 42]:

- Observations & Measurements (O&M): Standard models and XML schema for encoding observations and measurements from a sensor, both archived and in real time;
- Sensor Model Language (SensorML): Standard models and XML schema for describing sensor systems and processes associated with sensor observations in order to provide information required for the discovery of sensors, location of sensor observations, processing of low-level sensor observations, and listing of taskable properties, as well as supporting on-demand processing of sensor observations;
- Transducer Model Language (TransducerML or TML): A conceptual model and XML schema for describing transducers and supporting real-time streaming of data to and from sensor systems;
- Sensor Observations Service (SOS): A standard Web service interface for requesting, filtering, and retrieving observations and sensor system information as the intermediary between a client and an observation repository or a near real-time sensor channel;
- Sensor Planning Service (SPS): A standard Web service interface for requesting user-driven acquisitions and observations as the intermediary between a client and a sensor collection management environment;
- Sensor Alert Service (SAS): A standard Web service interface for publishing and subscribing to alerts from sensors; and
- Web Notification Services (WNS): A standard Web service interface for asynchronous delivery of messages or alerts from SAS and SPS Web services and other elements of service workflows.

As the OGC has identified the need for standardized interfaces for sensors in the WoT, the OGC has created a new Standards Working Group (SWG) on the sensor Web interface for the IoT. The sensor Web interface for the IoT SWG aims to develop such a standard based on existing WoT portals with consideration of the existing OGC Sensor Web Enablement (SWE) standards. This group will develop a candidate standard for access to sensor observations including location information well-suited to IoT and WoT deployment environments.

- **oneM2M**

Considering the increasing momentum for a standard system-level M2M architecture, seven of the world's leading ICT SDOs (i.e., ARIB and TTC of Japan, ATIS and TIA of the USA, CCSA, ETSI, and TTA of Korea) have launched a new global organization, called OneM2M, to ensure the most efficient development of M2M communications systems [43]. The new organization will develop specifications to ensure the global functionality of M2M, allowing a range of industries to effectively take advantage of the benefits of this emerging technology.

This sub-section has introduced related activities from SDOs on the IoT and M2M. For M2M, 3GPP/3GPP2 and ETSI have produced relevant standards and continued the work for considering many application areas. Dedicated groups on the IoT have also been established to enhance capabilities in a wide range of scope from the M2M concept. Standardization activities in specific areas are aligning in the umbrella of the IoT for a more synergic approach. A new approach for a global standard among SDOs is emerging and will become more and more important in terms of interoperability.

### 3.9.6. Conclusion

This section has introduced the concept and fundamental characteristics of the IoT and investigated the key technologies and requirements for the evolution from M2M to an IoT/WoT, considering the vision and technology trends. Major application fields of the IoT have also served to reveal the significant potential impact to other industries using ICT. Based on relevant activities to develop architectures from the ITU-T and related research projects, this section has shown some of the architectural models to identify related functionalities. Many standards on the IoT are developing concurrently in related SDOs, and these standardization efforts are becoming increasingly important due to the necessity of global standards for interoperability among various solutions. To realize the IoT, leading technologies are expected to become highly integrated, such as autonomic networking, data mining and decision-making, security and privacy protection, as well as cloud computing, with technologies for advanced sensing and actuation varying according to specific use cases.

**References**


1. Luigi Atzori, Antonio Iera, Giacomo Morabito, “The Internet of Things: a survey” *Computer Networks*, vol.54, issue 15, October 2010, pp.2787-2805.
2. *Overview of Internet of Things*, ITU-T Y.2060, June 2012.
3. *Framework of object-to-object communication for ubiquitous networking in Next Generation Network*, ITU-T Y.2062, March 2012.
4. Disruptive Technologies Global Trends 2025, *Appendix F: The Internet of Things (Background)*, SRI Consulting Business Intelligence, 2010.
5. *Overview of ubiquitous networking and of its support in NGN*, ITU-T Y.2002, October 2009.
6. Gyu Myoung Lee, Noel Crespi, “Shaping Future Service Environments with the Cloud and Internet of Things: Networking Challenges and Service Evolution,” *Lecture Notes in Computer Science (LNCS)* 6415, October 2010, pp.399-410.
7. Mathieu Boussard, Benoit Christophe, Olivier Le Berre, Vincent Toubiana, “Providing user support in Web-of-Things enabled smart spaces,” *Proceedings of the 2nd International Workshop on Web of Things*, no.11, June 2011.
8. Patrick Guillemin, Peter Friess, *et al*., “Internet of Things - Strategic Research Roadmap,” The Cluster of European Research Projects on the Internet of Things (CERP-IoT) Strategic Research Agenda (SRA), September 2009.
9. Dave Evans, “The Internet of Things – How the Next Evolution of the Internet is Changing Everything,” *White Paper, Cisco*, April 2011.
10. “More than 50 billion connected devices,” *Ericsson White Paper*, February 2011.
11. Andrew Brown, John Moroney, “A Brave New World in Mobile Machine-to-Machine (M2M) Communications. Strategy Analytics,” *Forecast and Outlook Snapshot*, July 2008.
12. *What is M2M communications*, viewed 1 October 2012, <http://www.m2mcomm.com/about/what-is-m2m/index.html>.
13. *M2M vs. Internet of Things*, August 2010, viewed 1 October 2012, <http://weblog.cenriqueortiz.com/internetofthings/2010/08/02/m2m-vs-internet-of-things/.
14. Accenture, *Sensor telemetry*, 2005, viewed 1 October 2012, <http://www.accenture.com/SiteCollectionDocuments/PDF/sensortelemetry.pdf>.
15. Dominique Guinard, Vlad Trifa, Friedemann Mattern, Erik Wilde, “From the Internet of Things to the Web of Things: resource oriented architecture and best practices,” *Architecting the Internet of Things*, *Springer*, 2011, pp.97-129.
16. *Framework of Web of Things*, *work in progress*, ITU-T Y.2063, July 2012.
17. Dennis Pfisterer, Kay Romer, Danel Bimschas, Oliver Kleine, Richard Mietz, Cuong Truong, Henning Hasemann, Alexander Kroller, Max Pagel, Manfred Hauswirth, Marcel Karnstedt, Myriam Leggieri, Alexandre Passant, Ray Richardson, “SPITFIRE: Toward a semantic Web of Things,” *IEEE Communications Magazine*, vol.49, issue 11, November 2011, pp.40-48.
18. Tridium “Web of Things” White paper, September 2009.
19. Zach Shelby “Embedded Web services,” *IEEE Wireless Communications*, vol.17, no.6, December 2010, pp.52-57.
20. *The social Web of Things – a social network for your devices*, February 2011, viewed 1 October 2012, <http://www.ericsson.com/thinkingahead/idea/110217_social_network_for_you_1968920151_c>.

21. Antonio Pintus, Davide Carboni, Andrea Piras, “Paraimpu: a Platform for a Social Web of Things,” *the international World Wide Web (WWW) conference*, Demos Track, April 2012, pp.401-404.
22. Les Instituts Carnot, “Smart Networked Objects and Internet of Things, which takes an ever broader view of the practice and potential of IoT,” *white paper,* v1.1, January 2011.
23. INFSO D.4 Networked Enterprise & RFID INFSO G.2 Micro & Nanosystems, in co-operation with the Working Group RFID of the ETP EPOSS, “Internet of Things in 2020, Roadmap for the Future,” Version 1.1, 27 May 2008.
24. Dieter Uckelmann, Mark Harrison, Florian Michahelles, “An architectural approach towards the future Internet of things,” *Architecting the Internet of Things, Springer*, 2011, pp.1-24.
25. InterDigital, “Standardized M2M Software Development Platform,” White Paper, 2011.
26. Fundacion de la Innovacion Bankinter, “The Internet of Things – in a connected world of smart objects,” 2011, viewed 1 October 2012, <http://www.fundacionbankinter.org/system/documents/8189/original/XV_FTF_Interneto_of_things.pdf>.
27. Michele Zorzi, Alexander Gluhak, Sebastian Lange, Alessandro Bassi, “From today’s Intranet of Things to a future Internet of Things: A wireless-and mobility-related view,” *IEEE Wireless Communications*, vol.17, no.6, December 2010, pp.44-51.
28. “Internet of Things. Pan European Research and Innovation Vision,” European Research Cluster on the Internet of Things, October 2011, viewed 1 October 2012, <http://www.internet-of-things-research.eu/pdf/IERC_IoT-Pan%20European%20Research%20and%20Innovation%20Vision_2011_web.pdf>.
29. Jayavardhana Gubbi, Rajkumar Buyya, Slaven Marusic, Marimuthu Palaniswami, “Internet of Things (IoT): a vision, architectural elements, and future directions,” *The Computing Research Repository (CoRR)*, July 2012.
30. Internet of Things – Architecture (IoT-A), “Project Deliverable D1.2 – Initial Architectural Reference Model for IoT,” viewed 1 October 2012, <http://www.iot-a.eu/public/public-documents>.
31. FI-WARE, “Internet of Things (IoT) Services Enablement,” viewed 1 October 2012, <http://forge.fi-ware.eu/plugins/mediawiki/wiki/fiware/index.php/Internet_of_Things_%28IoT%29_Services_Enablement>.
32. De-Li Yang, Feng Liu, Yi-Duo Liang, “A survey of the Internet of Things” *Atlantis Press*, 2010, pp.358-366.
33. Krishnan V, Bhaswar Sanyal, “M2M technology: challenges and opportunities” *white paper, Tech Mahindra*, 2010.
34. Kim chang, Anthony Soong, Mitch Tseng, Zhixian Xiang, “Global wireless machine-to-machine standardization,” *IEEE Internet Computing*, vol.15, issue 2, March 2011, pp.64-69.
35. ETSI website, http://www.etsi.org/WebSite/homepage.aspx.
36. ITU-T IoT-GSI website, http://www.itu.int/en/ITU-T/gsi/iot/Pages/default.aspx.
37. ITU-T FG-M2M website, http://www.itu.int/en/ITU-T/focusgroups/m2m/Pages/default.aspx.
38. OMA website, http://www.openmobilealliance.org/.
39. Internet-of-Things Architecture (IoT-A), “Project Deliverable D3.1 - Initial M2M API Analysis,” viewed 1 October 2012, <http://www.iot-a.eu/public/public-documents>.
40. IETF WGs website, http://datatracker.ietf.org/wg/.
41. Scott Fairgrieve, “Sensor Web standards and the Internet of Things,” *Proceedings of the 2nd International Conference on Computing for Geospatial Research & Applications*, no.73, May 2011.
42. OGC, Sensor Web Enablement DWG, http://www.opengeospatial.org/projects/groups/sensorwebdwg.
43. OneM2M website, http://www.onem2m.org.

## 3.10 Broadcasting

### 3.10.1. Background

Regulators, spectrum managers and broadcasters are faced with the question how to continue and extend the delivery of broadcasting services and introduce new broadcasting services in a frequency efficient and cost effective way, taking into account the following issues:

- local market requirements;
- existing transmission networks and receivers;
- alternative means of content delivery, including IP broadband, via mobile, fixed and satellite networks;
- regional and international regulatory requirements regarding the use of the frequency spectrum and in particular the impact of decisions adopted at the WRC-121;
- existing broadcasting transmission standards and future developments;
- demands of spectrum from other than broadcasting services.

Two main developments in terrestrial broadcasting will determine the trends in audio and television broadcasting:

- The fast expansion of high capacity data networks, offering consumers broadband Internet access. The Internet will be an increasingly important means of delivery of audio-visual content, including broadcasting.
- The continuing evolution of digital broadcast technology, resulting in a considerable increase of the capacity in the transmitted bandwidth and enabling more services, better picture quality and improved coverage.

### 3.10.2. Broadcasting services

Broadcasting services are by their nature downlink transmissions with programmes in a time sequence determined by the broadcaster (so called linear broadcasting). Enhanced broadcasting services complement the traditional broadcasting services and offer non-linear services (in an order and at time determined by the viewer) by means of interactivity, time-shifted viewing and continued reception at any location.

Enhanced broadcasting services could be offered by terrestrial broadcasting network, cable, IPTV and satellite networks in combination with broadband networks; so called hybrid broadcast-broadband (HBB) services. In addition, some delivery means can offer enhanced broadcasting to a certain extent. For instance DTTB can offer mobile and portable reception, MTV handheld reception and cable TV and IPTV may offer video-on-demand services.

- **Enhanced television broadcasting**

Enhanced broadcasting services are developed around three concepts:

- TV anytime, aiming at watching a specific programme at the time by choice of the viewer. Time shifted viewing is in particular of interest for shows, documentaries, movies etc., but a relative short time shift for sports and news programmes is also popular.
- TV anywhere, aiming at watching the broadcast service not only in the living room, but also in other rooms, on the move, etc. Mobile devices like smart phones and tablet computers are used for this application.
- Interactivity, aiming at contributing or reacting by the viewer to a specific programme, demanding for additional information regarding the programme or receiving programmes or information of particular interest.

TV anytime

Broadcast services are programmed in a linear way, but consumers may wish to watch the programmes at the time of their convenience, which could be time shifted from the broadcast transmission. There are basically three ways to realize time shifted viewing:

- Personnel video recorder (PVR). Programmes can be recorded on a hard disk and watched later. The provision of an electronic programme guide (EPG) could facilitate the recording functions considerably.
- Catch-up TV services via the open Internet. Catch-up TV services are watched at computers, smart phones and tablet computers, but also on television screens if the receiving set is equipped with facilities for Internet connection. So called connected TVs or hybrid broadcastbroadband (HBB) devices combine broadcast and

broadband delivery in the TV receiver and offer among others catch-up services (see also the section below on interactivity). Public fixed and mobile networks in combination with domestic WLAN networks will be necessary for uplink and downlink transmission of the catch-up services.
- Catch-up TV services as part of a video-on demand offer. Providers of digital cable TV services and IPTV services may offer also catch-up TV services as part of a video-on-demand offer.

TV anywhere

Consumers may wish to watch their favourite programmes anywhere, on route, in the living room and in other rooms. In addition to the main TV set, second sets and other types of receivers such as pc, smart phone and tablet computer are used. Reception of the programme on the latter two devices is realized by means of IPTV and broadband TV via public fixed and mobile networks in combination with domestic WLAN networks. Alternatively, DTTB or dedicated mobile TV networks (MTV) could be used if the devices are equipped with the appropriate systems.

Interactivity

Consumers may wish to participate actively in the programme by means of voting, giving comments, receiving additional information or wish to receive video-on-demand programmes. Also programme independent information may be offered such as news, e-government and e-learning services as well as commercial applications for ordering good or services. For this kind of interactive services, a return path (upload) is necessary and often also a second download path to distribute the requested information.

A summary of the enhanced television broadcasting concepts is shown on Table 3.1.

**Table 3.1: Summary of enhanced television broadcasting concepts**

| Enhanced broadcasting | Delivery | Terminal devices (must be equipped to receive the corresponding transmission standard) |
|---|---|---|
| **TV anytime** | • Broadcast (DTTB)<br>• Hybrid broadcast-broadband<br>• Broadband | • PVR/TV set<br>• TV set *); tablet computer; smart phone<br>• PC; tablet computer; smart phone |
| **TV anywhere** | • Broadcast (DTTB)<br>• Broadcast (MTV)<br>• Broadband | • TV set; car TV set; tablet computer; smart phone<br>• Car TV set; tablet computer; smart phone<br>• PC; tablet computer; smart phone |
| **Interactivity** | • Broadcast (DTTB)<br>• Broadcast (MTV)<br>• Hybrid broadcast-broadband<br>• Broadband | • TV set (local interactivity)<br>• Tablet computer; smart phone<br>• TV set *); tablet computer; smart phone<br>• PC; tablet computer; smart phone |
| | | *) With Internet connection |

- **Television broadcasting development**
- In an increasing number of countries all TV services will be in HD quality.
- Screen sizes will increase and for large screens (> 50 inch) the presentation format 1080p/50 or 60 may be implemented on some DTTB networks.
- UHDTV will be implemented in some countries, with advanced compression systems. Implementation on DTTB networks is not expected.
- A new, twice as efficient compression system called HEVC/MPEG-H/H.265 will be available. The system will have a two times higher coding efficiency than MPEG4. Initially it may be used with UHDTV services. It is also likely to be included in the specifications of DTTB standards.
- Second generation transmission systems will be implemented in more and more countries to provide sufficient capacity on the DTTB networks in order to:

– deliver an attractive HDTV service package;
– compensate the reduction of the UHF TV band, due to the introduction on IMT services.

- A single global new generation of standard, referred to as FOBTV, has been developed with the aim to achieve compatible DTTB standards worldwide.
- The MTV market prospective is variable. Many systems exist, either as dedicated MTV system, or as part of a DTTB transmission. In addition, multimedia services via mobile communication networks (3G and 4G) show very high growth figures.
- More services, with better picture quality (including HDTV) and better reception quality will be implemented on the terrestrial platform. In countries where the UHF TV band will be limited to 694 MHz, the following activities may take place:

– major frequency re-plannning to accommodate the transmission of the services into a reduce frequency band;
– application of second generation transmission standards;
– re-engineering of transmitting stations;
– organizing a transition period to allow viewers to buy new receivers;
– communication campaigns to inform the public about the required changes in receiving installations.

- **Enhanced audio broadcasting**

The service concepts in audio broadcasting follow similar patterns as in television broadcasting. However, the "anywhere" concept is much more developed in audio broadcasting. Reception of analogue audio broadcasting in FM and AM and DTAB takes place almost everywhere: with portable receivers or high-end audio-sets in every room in the house, with car radios while driving, outside and in public places with small pocket radios and mobile phones and in waiting rooms and shopping centres by means of central audio installations.

Streaming via the Internet is becoming a very important means of delivery. Thousands of radio stations from all over the world can be received in good quality with radio receivers equipped with Internet access, or with mobile phones and computers.

Interactivity and hybrid broadcast-broadband (HBB) is also developing in audio broadcasting. HBB radio receivers with a screen for displaying additional personalised information appear on the market. RadioDNS (Domain Name Service) is an initiative to help broadcasters to offer HBB services with the aim that the listener is unaware that the linear broadcasting services and the personalised broadband services are combined. This is achieved by making use of existing identifiers of the radio station used with, e.g. FM-RDS, DAB, DRM or IBOC and to locate the IP delivered services of that station.

A summary of the enhanced audio broadcasting concepts is shown on Table 3.2.

**Table 3.2: Summary of enhanced audio broadcasting concepts**

| Enhanced broadcasting | Delivery | Terminal devices (must be equipped to receive the corresponding transmission standard) |
|---|---|---|
| **Radio anytime** | • Broadcast (DTAB)<br>• Hybrid broadcast-broadband<br>• Broadband (broadcaster's website) | • PVR/ audio set<br>• Radio set*); tablet computer; smart phone<br>• PC; tablet computer; smart phone |
| **Radio anywhere** | • Broadcast (AM/FM)<br>• Broadcast (DTAB)<br>• Broadcast (MTV)<br>• Broadband | • Any radio set: Hifi audio set, portable radio, car radio, tablet computer, smart phone, simple mobile phone<br>• Any radio set<br>• Car radio; tablet computer; smart phone<br>• PC; tablet computer; smart phone |
| **Interactivity** | • Broadcast (FM)<br>• Broadcast (DTAB)<br>• Broadcast (MTV)<br>• Hybrid broadcast-broadband<br>• Broadband | • FM radio with RDS (local interactivity)<br>• Radio set (local interactivity)<br>• Car radio; tablet computer; smart phone<br>• Radio set*); tablet computer; smart phone<br>• PC; tablet computer; smart phone |
| | | *) With Internet connection |

- **Audio broadcasting developments**
- Many countries will introduce digital audio broadcasting for national and regional coverage in parts of the frequency band 174-230 MHz (Band III), when vacated by analogue television. Countries with DAB assignments or allotments in the Geneva 2006 Agreement will use these as a basis.
- In addition in many countries also digital audio broadcasting stations will be introduced in the LF, MF and HF bands in order to satisfy specific market requirements, such as coverage in low populated areas, international broadcasting and local broadcasting.
- More than one digital audio broadcasting system in different frequency bands or in the same frequency band may be in operation in the same country in order to satisfy the various market requirements. The availability of multi-standard and multi-band receivers is therefore an important condition for the development of digital audio broadcasting.
- An increasing number of digital audio broadcasting implementations will make use high efficiency source coding (e.g. DAB+). Eventually all transmissions with less efficient source coding will be replaced.

### 3.10.3. Broadcast and broadband delivery

It is expected that linear broadcasting services aimed at reception by the general public in a country or region will be enhanced with individualized services delivered by fixed (including domestic distribution by WLAN) and mobile networks. When broadband connections are available to a large part of the population, broadband will not only be the main means of delivery for individual non-linear broadcasting, but could also deliver linear broadcasting to the general public.

The relative importance of broadcasting and broadband delivery will be different from country to country depending on the market conditions and the regulatory situation. It may also be different for audio broadcasting and television services.

Figure 3-10-1 shows in a matrix the position of broadcast (BC) and broadband (BB) delivery with regard to the linear and non-linear broadcasting services.

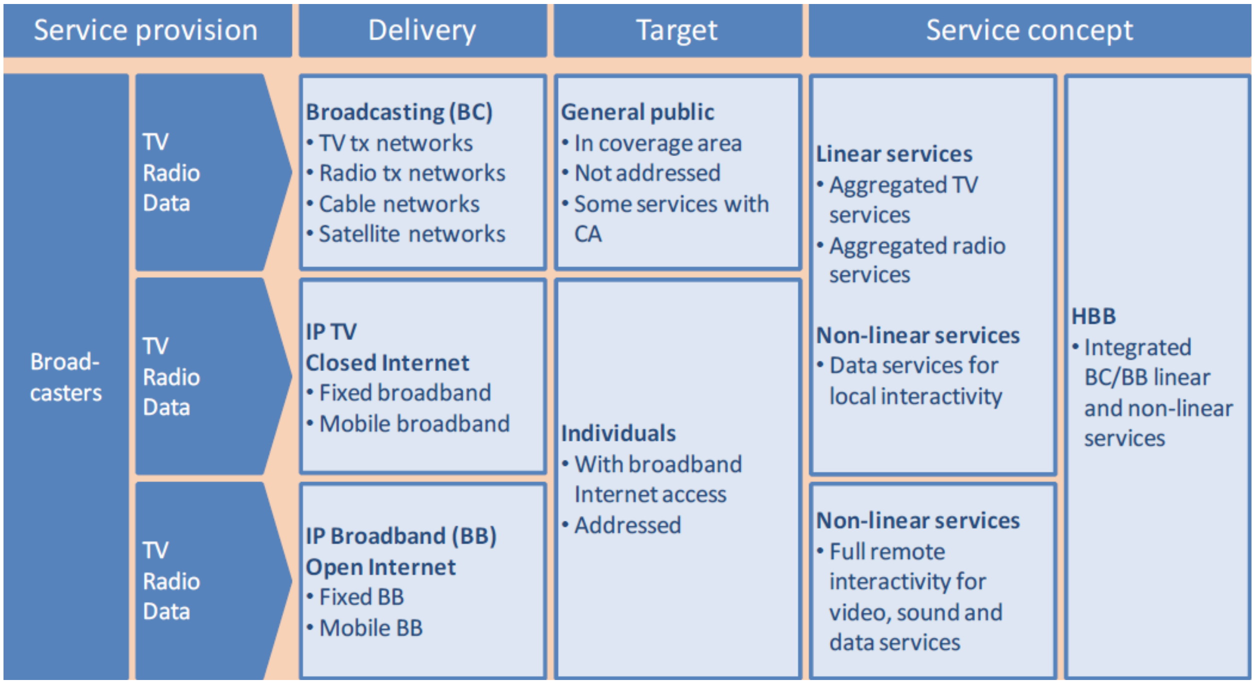


Figure 3-10-1 – Position of broadcast (BC) and broadband (BB) delivery (source: ITU)

The importance of broadband delivery is expected to increase and will enable integrated hybrid broadcast-broadband (HBB) services. It is not expected that broadband will replace broadcast as the main means of delivery for linear broadcasting to the general public, but it cannot be excluded on the long term. It will depend on national market conditions and regulatory situation.

**References**

1. ITU, "Trends in broadcasting: an overview of developments," February 2013.

## 3.11 Spectrum issues for developing countries

### 3.11.1. Background

Spectrum management is the process of regulating the use of radio frequencies to promote efficient use and gain a net social benefit. The term radio spectrum typically refers to the full frequency range from 3 kHz to 300 GHz that may be used for wireless communication. Increasing demand for services such as mobile telephones and many others has required changes in the philosophy of spectrum management. Demand for wireless broadband has soared due to technological innovation, such as 3G and 4G mobile services, and the rapid expansion of wireless internet services.

The International Telecommunication Union (ITU) is the part of the United Nations (UN) that manages the use of both the RF Spectrum and space satellites among nation states. The Plenipotentiary Conference is the top policy-making body of the ITU, meeting every four years in order to set the Union's general policies. The ITU is divided into three Sectors: the Radiocommunication Sector (ITU-R) determines the technical characteristics and operational procedures for wireless services, and plays a vital role in the Spectrum Management of the radio-frequency; ITU-R Study Group 1 is the Spectrum Management study group; the Telecommunication Standardization Sector (ITU-T) develops internationally agreed technical and operating standards; and the Telecommunication Development Sector (ITU-D) fosters the expansion of telecommunications infrastructure in developing nations throughout the world, that make up two-thirds of the ITU's 191 Member States. The ITU Radio Regulations set a binding international treaty governing the use of the radio spectrum by some 40 different services.

The radio-frequency spectrum constitutes the raw material of any radiocommunication system, and is an intangible asset linked to the sovereignty of the State and the exercise of regal powers. This particular asset may be relatively scarce in some instances. The cause of its scarcity is to be found not only in institutional mechanisms, but also in a growing demand for uses resulting from technical progress. This demand comes up against the fact that there is an increasingly narrow bottleneck in the availability of the resource.

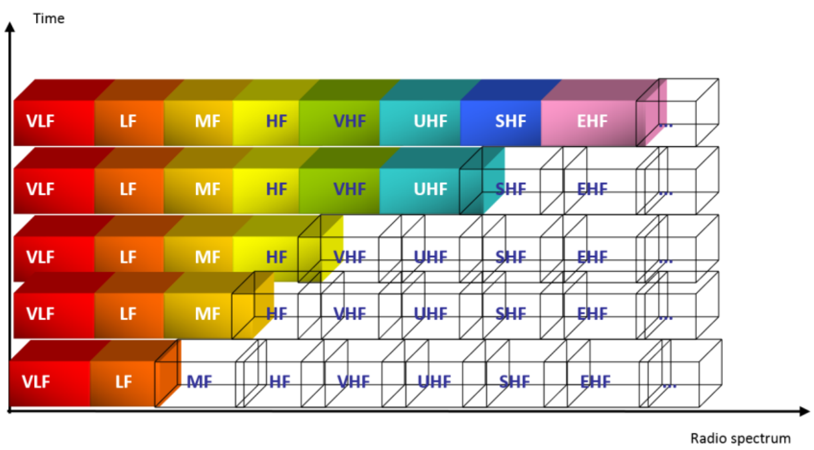



Figure 3-11-1 –Scarcity of radio frequencies

The following factors contribute to the scarcity of frequencies and increased spectrum access costs:

- The deregulation and liberalization of electronic communication markets
- The privatization and "merchandizing" of the public domain
- Awareness of the value of the spectrum
- Worldwide competition between multinational operators.

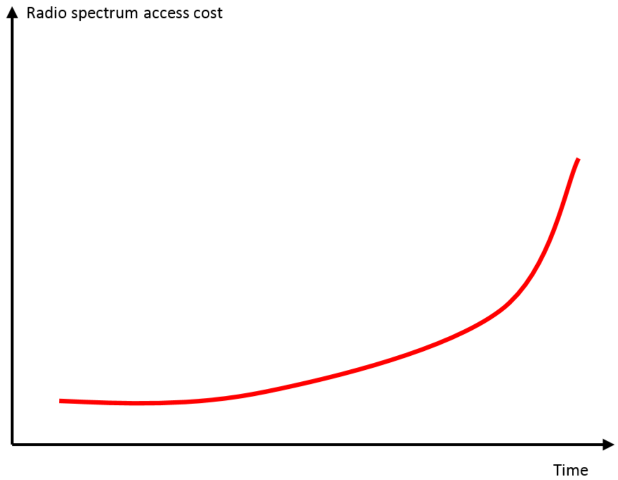



Figure 3-11-2 – Increase in radio spectrum access costs

It must be noted that hitherto reflection concerning this natural resource has focused mainly on the case of the developed countries. The developing countries have long been left more or less on the fringe of the debates that took place in the technical, legal, economic and political fields.

This divergence of interest between developed and developing economies is explained by the very different structural and institutional contexts in which the uses of the spectrum resource have evolved.

Debates are nevertheless now beginning to run along much the same lines in all countries of the world, regardless of the legal or institutional regimes in place. They proceed from the same premise, that the challenges in frequency management are no longer simply technical and administrative, but also economic and financial. The financial approach and market strategies are steadily imposing themselves on all players in the radiocommunication sector, especially regulators and operators, who are finding themselves obliged to move from an administrative approach to economic and financial approaches.

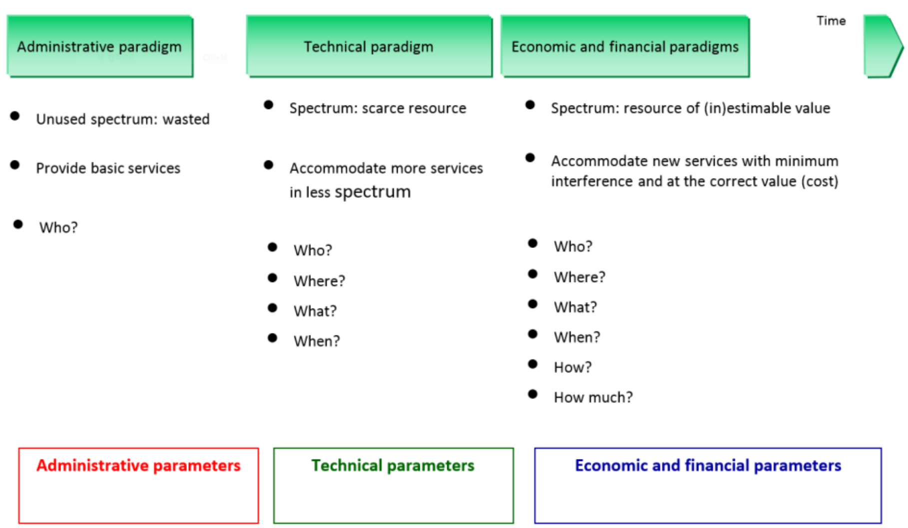



Figure 3-11-3 –Paradigm shift

- **Increasing recourse to market mechanisms**

This profound paradigm shift is increasingly encouraging the adoption of new frequency allocation mechanisms. Different methods exist in cases where demand for frequencies exceeds supply. Traditionally, public authorities have often allocated frequencies for specific applications, and then assigned parts of the spectrum to entities responsible for using them for specific purposes based on the "first come, first served" principle. This approach is fast, practical and uncostly, but has its limits in today's competitive environment.

Indeed, the limited resources required to operate a telecommunication service (radio spectrum, numbers, rights of way) should be divided up among operators in a manner that is equitable, effective, and serves the public interest.

To meet this concern, the WTO reference document on basic telecommunications (1997) promoted the emergence of new allocation methods. Any procedures for the allocation and use of scarce resources, including frequencies, will be carried out in an objective, timely, transparent and non-discriminatory manner (paragraph 6).

Players in the radiocommunication sector are thus making increasing use of market mechanisms, such as auctions and secondary trading, in order to optimize the value of the radio spectrum. Such optimization is now becoming both necessary and sought after by public authorities for several reasons:

- To encourage an effective use of this resource which is not produced, is limited, and is in some cases scarce
- The frequency spectrum has become an important means to develop countries' telecommunications
- The budgetary income generated by the spectrum can contribute to countries' economic development
- Income from frequencies must contribute to improving the means used for spectrum management (monitoring, spectrum management information system, …) and make it possible to fund refarming operations.

### 3.11.2. Guidance on the regulatory framework for national spectrum management

- **The international context**

The telecommunication sector, including radiocommunications, is organized internationally within the framework of the International Telecommunication Union (ITU), which provides the basic framework for the global coordination and management of the radio-frequency spectrum. In between ITU and the national administrations, two other kinds of organizations, regional organizations and specialized international organizations, are also involved in spectrum management, at either regional or global level.

At the regional level, organizations have been founded that bring together administrations, in some cases associating industry or radiocommunication operators. Their aim is to establish common positions in preparation for ITU decisions, to harmonize national frequency allocations within the relatively flexible framework set by ITU so as to facilitate the coordinated introduction of new services, and to harmonize the standards and procedures for certification of equipment with a view to its free circulation and use in the countries concerned. This is the case in particular for the European Conference of Postal and Telecommunications Administrations (CEPT), and to a lesser extent for the Inter American Telecommunication Commission (CITEL), the Asia-Pacific Telecommunity (APT) and the Arab Council of Ministers for Telecommunication and Information, which in pursuing these objectives intend to promote the emergence of regional markets and hence to accelerate the development of radiocommunication services.

At the global and regional levels, specialized international organizations also exist in sectors of activity that use radiocommunications and are therefore dependent on spectrum availability: civil aviation, the maritime sector, meteorology, broadcasting, radio amateurs, radio astronomy and research.

The World Trade Organization, within the framework of the General Agreement on Trade in Services (GATS), while recognizing the sovereign right of States to manage the frequency spectrum in terms of their own objectives, works to develop the instruments required so that exercise of that right does not in fact result in barriers to trade in services between its members.

In this context, the establishment of standards at regional and global levels constitutes one of the fundamental means of promoting efficient and economical use of the spectrum and the development of radio services.

(1) International principles governing spectrum use

The radio-frequency spectrum is a non-depletable but limited natural resource available in all countries and in outer space. Since any transmitting radio station may cause harmful interference to spectrum uses on Earth or in space, the spectrum is a common resource of mankind that requires rational management by a treaty level agreement among all countries. In that spirit, ITU has been drawing up legal instruments for over a century, so that spectrum use is based on the following fundamental principles set forth in the ITU Constitution (CS):

- “while fully recognizing the sovereign right of each State to regulate its telecommunication...” (ref CS 1), “... to avoid harmful interference between the radio stations of different countries” ref CS 11);

- "… to improve the use made of the radio-frequency spectrum for radiocommunication services and of the geostationary-satellite and other satellite orbits" (ref CS-12);
- to "facilitate the worldwide standardization of telecommunications, with a satisfactory quality of service" (ref CS-13), and "... to harmonize the development of telecommunication facilities, ... with a view to full advantage being taken of their possibilities" (ref CS-15);
- to "foster international cooperation and solidarity ..." (ref CS-14).

The ITU Radio Regulations (RR) constitutes the principle regulatory framework within which States undertake to operate radio services and the basic tool for international spectrum use. They have international treaty status and are periodically reviewed (about every three years) by World Radiocommunication Conferences (WRC), which are attended by most ITU Member States.

The RR specify, inter alia, the frequency bands allocated to radio services and the regulatory conditions and procedures that administrations must follow for implementing radio stations providing those services. The guiding principle underlying all RR provisions is that new uses must avoid causing harmful interference to the services provided by stations using frequencies assigned to them in accordance with the RR and recorded favourably in the Master International Frequency Register (MIFR).

The RRs, as drawn up by successive WRCs in the past years, aims to allow each country the greatest possible flexibility with regard to spectrum use. In particular, the Table of Frequency Allocations (RR Article 5) authorizes several radiocommunication services in each band; those services are not necessarily compatible locally, but each country can select those it wishes to implement on its territory. The RR's regulatory provisions and procedures then enable each country to coordinate, as required, the stations providing the services selected with those of other countries that may be affected, thus maximizing the efficient utilization of the spectrum.

This relatively flexible framework has the advantage of respecting the wide range of countries' spectrum needs and their sovereign right to meet those needs as long as it does not place undue constraints on other countries. It has the disadvantage of limiting economies of scale and the capacity for interoperability required to develop radiocommunications, in particular within the framework of worldwide services or those intended for the general public (e.g. mobile telephony, satellite broadcasting). For this reason, a major effort has been made in the past years to harmonize spectrum use at regional, or even global level, in particular with regard to mobile telephony. The activity towards harmonization has been to identify specific frequency bands for applications, corresponding to specific standards. The purpose of this harmonization is to increase economy of scales and decrease interference and incompatibilities.

(2) Multilateral agreements

International Telecommunication Union (ITU)

The agreements, which in fact are a treaty binding the Member States within the framework of ITU, lay the foundation for spectrum management worldwide. ITU international agreements recognize that utilization of the radio-frequency spectrum is a matter of State sovereignty, but that to be efficient it must be regulated. They are the basic global instruments with which, States, in ratifying such a work, undertake to respect common rules for sharing and using the spectrum, the goal being efficient utilization and equitable access.

The ITU instruments relevant to spectrum management are the Constitution (CS), the Convention (CV) and, mainly, the Radio Regulations (RR). These instruments are only binding on the Member States among themselves.

Article 6 No. 37 of the CS states "The Member States are bound to abide by the provisions of this Constitution, the Convention and the Administrative Regulations in all telecommunication offices and stations established or operated by them which engage in international services or which are capable of causing harmful interference to radio services of other countries, except in regard to services exempted from these obligations in accordance with the provisions of Article 48 of this Constitution".

And further, No. 38 of the same article states "The Member States are also bound to take the necessary steps to impose the observance of the provisions of this Constitution, the Convention and the Administrative Regulations upon operating agencies authorized by them ..."

Compliance with these instruments therefore presupposes that each State may also take, to the extent outlined above, the measures necessary (legislation, regulations, clauses in licences and authorizations) to extend into the domestic regime the obligations of such instruments to other spectrum users (operators, administrations, individuals, etc.).

### 3.11.3. Managing the radio spectrum in developing countries

Moving management of the radio spectrum closer to markets is long overdue. The radio spectrum is a key component of the telecommunications infrastructure that underpins the information society. Spectrum management, however, has not kept up with major changes in technology, business practice, and economic policy during the last two decades. Traditional spectrum management practice is predicated on the spectrum being a limited resource that must be apportioned among uses and users by government administration. For many years this model worked well, but more recently the spectrum has come under pressure from rapid demand growth for wireless services and changing patterns of spectrum use. This has led to growing technical and economic inefficiencies, as well as obstacles to technological innovation. Two alternative approaches are being tried, one driven by the market (tradable spectrum rights) and another driven by technology innovation (spectrum commons). Wholesale replacement of current practice is unlikely, but the balance between administration, tradable rights, and commons is clearly shifting. Although the debate on spectrum management reform is mainly taking place in high-income countries, it is deeply relevant to developing countries as well. Indeed, to the extent that developing countries have less investment in wireless infrastructure than do many developed countries, adoption of more efficient spectrum management regimes may be easier and have larger payoffs (in relative terms) than in developed countries.

Developing countries comprise, by definition, all countries with low or middle average per capita incomes. These are about 150 countries in all continents, accounting for 85 percent of the world's population and about one-half of its GDP at purchasing power parity or 30 percent at current exchange rates. Despite the common label, this is a very heterogeneous group. Per capita annual incomes range from about $100 in Ethiopia to nearly $10,000 in Argentina, and sizes go from 1.3 billion in China to a few thousand in some Pacific islands. There is also major variation within individual countries. Modern economic sectors (including telecommunications in some countries) may perform to world standards yet coexist with a subsistence agricultural economy. Prosperous groups live next to large segments of the population in abject poverty.

Communication and information services in the developing world have experienced explosive growth. Between 1980 and 2005 the number of phones (fixed and mobile) multiplied 30-fold (while population grew by one-half and real GDP more than doubled) and their share in the world's stock of phones more than tripled to about 60 percent. This largely resulted from economic and sectoral reforms, starting in the late 1980s and gradually extending to most developing countries, which led to private-led, increasingly competitive telecommunications markets.

Yet about one-half of all developing countries still have closed or only modestly open markets. Moreover, significant differences remain among and within developing countries.

Fast growth in large emerging markets, notably China, India, and Brazil, masks slower development in other economies. Progress has been made reaching out to rural areas and the urban poor, but in many countries these groups still lag in relative terms. More advanced communication and information services have become available through the Internet, but are only reaching the better-off population groups.

In most developing countries, the radio frequency spectrum is managed along the lines of traditional government administration. Some spectrum authorities have become very competent, and a few now play lead roles developing regulatory capacity in their regions. But in most countries spectrum management performs rather poorly. One or more of the following deficiencies are commonly found:

- Many countries fail to make detailed country-specific allocations in their national frequency plans, creating uncertainty for users and investors.
- Spectrum needed to provide new services (e.g., mobile, fixed wireless) is typically made available initially to only one operator, and gradually to a few more, resulting in artificial scarcity and high spectrum prices.
- Spectrum occupied in the cities is often under-utilized in rural areas.
- Spectrum allocation and use may be different across countries, and cross-border interference may arise.
- Large spectrum parcels are in the hands of public sector entities, including the military, and used only sparsely.
- Day-to-day administration is constrained by incomplete records of existing authorizations, limited capability to monitor and enforce compliance,3 slow processing of new applications, and shortage of skilled staff and data processing facilities.
- Unpredictability of the spectrum regime adds to regulatory risk and discourages investment.
- Unclear rules and lack of transparency create opportunity for political interference and corruption.

- While the primary objective of government administration should be to protect spectrum users from harmful interference by one another, in practice spectrum management is often viewed as a source of revenue for the government.

Efforts to improve spectrum management have mainly focused on day-to-day administration. For example, large investments are made in monitoring facilities that often go beyond critical needs and exceed the authorities' human resources and enforcement capabilities. In the absence of spectrum policy changes and constrained by institutional capacities, these efforts tend to have limited impact. But a growing number of developing countries are trying to do more. Auctions are now routinely used in many countries to assign spectrum when demand exceeds supply.5 Spectrum refarming is making space for broadband wireless services using third-generation mobile technology. Some spectrum is being released or reallocated for unlicensed use.

Limited improvements of an essentially outdated model are unlikely to suffice. Further change in the spectrum management regime will largely be driven by current domestic issues, new technologies with potential to accelerate progress toward priority development objectives, and awareness of growing experience in other countries. Current high-visibility issues include moving toward third-generation mobile services, facilitating the deployment of broadband wireless technologies, planning the transition to digital television broadcasting, and recovering military spectrum for commercial use. But the scope of spectrum reform is broader, and solutions need to be designed that transcend particular applications.

What can developing countries do about the opportunities and challenges of spectrum reform?

In particular, how would the various approaches to spectrum management fare in poor countries with weak governance, incomplete infrastructure networks, large rural populations with minimal service, fast growth, and persistence of legacy equipment? How can countries make the transition from often poorly run government administration of the spectrum to a regime increasingly driven by markets and technology? How much effort should be invested in improving government administration of the spectrum? Would it not be better to improve administration rather than introduce new management models? What agencies could deal with harmful interference and resolve disputes? Is there danger that spectrum will be cornered by a few influential players? Who would pay for the cost of spectrum regulation as larger segments are released for unlicensed use? How can treasuries be weaned from the large rents they have grown accustomed to exact from spectrum licensees? How can spectrum policies be integrated with telecommunications and broadcasting reforms and with economic policy generally?

Some of these questions can be answered only in a particular country context and go beyond the scope of what can be achieved by a desk exercise.

### 3.11.4. Spectrum management approaches

- **Improving Traditional Government Administration**

Traditional spectrum management is predicated on the spectrum being a limited resource that must be apportioned among uses and users by the government. The primary objective of government administration is to protect spectrum users from harmful interference by one another.

Additional objectives are to achieve economic and technical efficiency of spectrum use, safeguard public services, and balance certainty to attract investment with flexibility to take advantage of change.

Features

- Government allocates spectrum among types of uses and establishes conditions of use
- Within each band, government assigns frequencies to individual users for exclusive or shared use
- Detailed technical and operating rules and standards prevents harmful interface

Advantages

- Mature practice, ample experience on which to draw
- Proven effective in preventing harmful interference
- Scope for some improvement over traditional practices

Limitations

- Increasingly unable to respond to demand growth, changing uses, and new technology
- Inflexibility and shortages slow down services competition, innovation, and growth
- Can result in major economic and technical inefficiencies
- Limited scope for improvement
- Excessive regulatory burden

- **Establishing Tradable Spectrum Rights**

Like traditional government administration, the tradable spectrum rights approach to management of the radio spectrum (a) is based on the premise that the spectrum is an inherently scarce resource that must be apportioned among competing uses and users and (b) focuses on protecting users from harmful interference. But responsibility for apportioning spectrum among uses and users is primarily delegated to the market rather than kept in the hands of the spectrum authority.

Features

- Government grants exclusive and transferable rights to individual users to use specific frequencies
- Rights holders may sell, lease, divide, or aggregate spectrum
- Rules and rights of use prevent harmful interference

Advantages

- Can correct for inefficient initial assignment and allocation
- Creates incentives for efficient use
- Accelerates response to changing technology and demand
- Enhance transparency and reduces opportunities for corruption
- Reduces regulatory burden

Limitations

- Few spectrum buyers and sellers can impede effective market development
- High transaction costs can discourage spectrum trades
- International agreements limit scope for liberalizing spectrum use
- Risk of market failures, mainly interference and anticompetitive trading
- Potential conflict with public policies, mainly fiscal, windfalls, service obligations, industrial

- **Developing a Spectrum Commons**

In contrast with the traditional government administration and the spectrum rights regime, both predicated on individual licenses conveying rights to use specific frequencies in a defined area, the commons approach is based on an open sharing of spectrum among users without guarantees of interference-free operation. Spectrum frequencies are not assigned to specific users, neither by a regulatory authority nor by the market, and it is generally left to the users and their equipment to avoid interfering with one another.

Features

- Spectrum is made available to all users
- Users are subject to minimal technical standards to limit interference
- Flexible usage rights with little or no restriction on user or technology
- No guarantee of interference-free operation

Advantages

- Encourages use of spectrum-efficient technologies
- Lowers entry barriers, enhances competition, facilitates innovation

- Reduces some forms of anticompetitive behavior
- Reduces regulatory burden

Limitations

- Risk that commons will be overused, resulting in reduced data rates
- Irreversibility of deregulation
- Loss of government control over spectrum and related revenues
- Commons possibly not as attractive for large investments as exclusive rights

### 3.11.5. Spectrum management system for developing countries (SMS4DC)

It is generally accepted that an effective telecommunication infrastructure is one of the essential drivers that enables a country to achieve successful social and economic development. Wireless telecommunication is especially important for developing countries because it will reduce the time and expense of installing copper or fibre networks in large rural areas. Therefore, an orderly management of the national use of the radio spectrum resource is crucial to obtain the maximum benefits. A number of administrations of developed countries are exploring the use of market methods to transfer responsibility for detailed spectrum management to industry and users.

However, these administrations, without exception, have the benefit of a long standing and strong foundation in traditional (so called command and control) spectrum management methods that enables them to create a technical and regulatory envelope within which the new methods can operate successfully and safely.

The International Telecommunication Union Telecommunication Development Bureau (ITU-BDT) can supply a computer program to assist the administrations of developing countries to perform their spectrum management responsibilities more effectively. This program is known as the Spectrum Management System for Developing Countries (SMS4DC). SMS4DC is intended to be a low-cost, entry-level spectrum management system; however, it is a very complex software tool with many technical features and functions. This document has been prepared by the ITU to provide an executive overview of the system for those intending to purchase and operate the software in their administrations or agencies.

It is emphasised that, for successful installation and operation of SMS4DC, the Administration should have in place existing legal, regulatory and technical mechanisms for national spectrum management. Also, while the system automates many of the technical processes, the final choice and decision for the frequency assignment remains with the engineer. Therefore, operating staff must have sufficient knowledge to understand the regulatory and technical processes that are the operational core of SMS4DC and to interpret correctly the results of the algorithms so that they can make good decisions.

Version 2.0 of the SMS4DC software has been designed to manage frequency assignments to the Land Mobile, Fixed and Broadcasting services and for frequency coordination of Earth stations (RR Appendix 7 procedures). While some assignment and interference analysis processes are unique to a particular service, there are several processes and tools that are applicable to all services. To avoid unnecessary repetition and to provide a logical approach, the common functions are grouped together into task-oriented sections. Where appropriate, brief explanatory information is given to assist in the understanding of the importance or purpose of the various tasks and what will be required from the Administration during installation and set-up.

The advanced features of SMS4DC include:

- User-friendly GUI
- Installable in networked environments
- Availability of different user access levels
- Employment of digital terrain model (DTM) on server or workstations
- Management of a shared hierarchical administrative database
- Integration of several propagation models
- Demonstration of calculation results on DTM
- Generation of new BR electronic notice form
- Interference calculation

- Frequency assignment
- Consideration of regional/national frequency allocation tables
- Consideration of regional agreements in technical calculations
- Frequency-planning capabilities
- Interface with BR-IFIC databases
- Generation of informative reports
- Employment of ITU modules for coordination contour calculation around Earth stations
- Frequency spectrum billing management
- Link to budget calculation
- User log for audit control
- English and French software interface
- Links to Argus (R&S) and Esmeralda (Thales) monitoring software
- Interface to Google™ Earth mapping

- **Main functions of SMS4DC**

Administrative Functions

- Relational database management
- Recording frequency application, frequency assignment, licensing, coordination data, import data from BRIFIC & SRS
- Producing electronic notices, print license, invoice & spectrum fee
- Security features: Multi level access enables system administrator to define users and groups with different access levels

Engineering Analysis Functions

- Enhanced analysis tools for frequency arrangement, assignment, coordination and interference calculation
- Propagation models based on ITU-R latest recommendations available at the time of development
- Coverage area, field strength, field strength contour, microwave link calculations, network coverage and best server calculation
- Azimuth, elevation and horizon elevation for earth stations
- Link to monitoring software

Geographic Map Display Function

- User friendly interface, displaying of DTM, capability of importing standard mapping formats including Globe map, displaying of other higher resolution maps and export to Google Earth
- Online latitude, longitude and altitude presentation, overlaying, Scrolling and Zooming functionality capability of handling vectors,
- Providing multiple entry functions, menu items, assigning new stations on map and searching and displaying a station or group of stations on map.

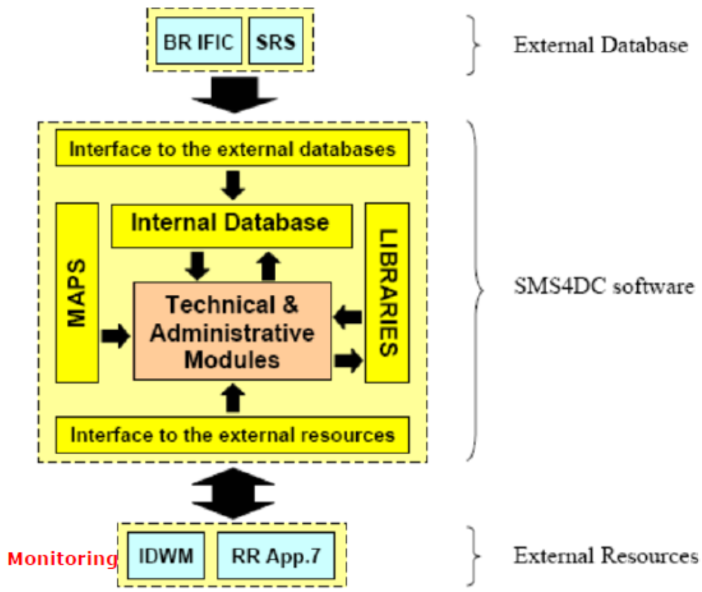


Figure 3-11-4 – Structure of SMS4DC

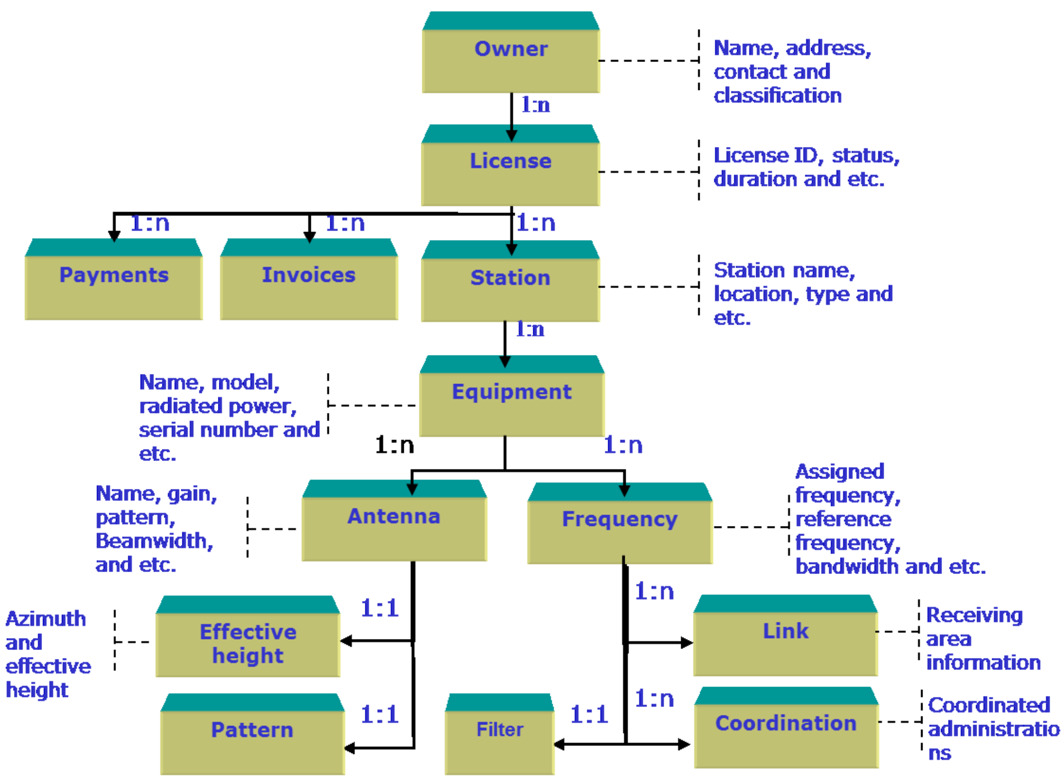


Figure 3-11-5 – User view of data (terrestrial)

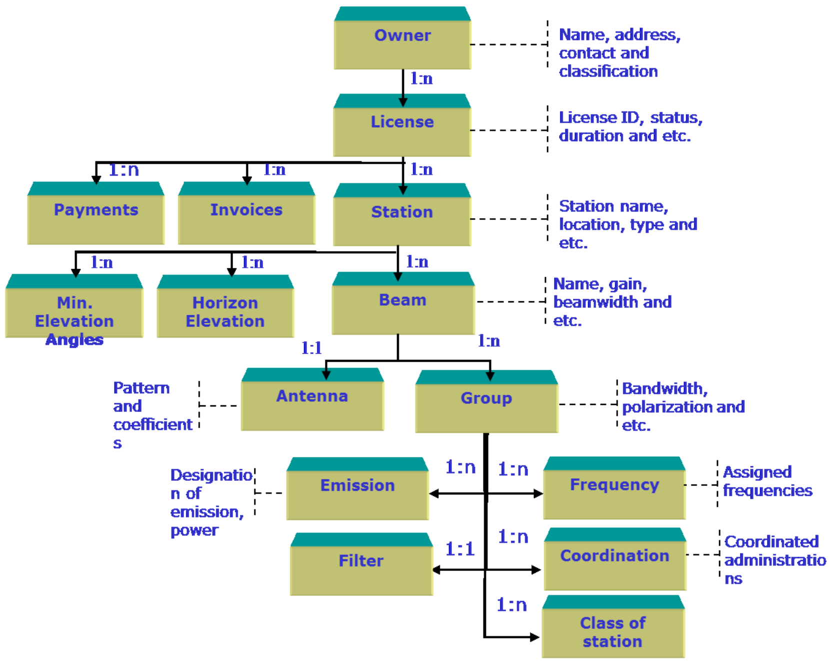



Figure 3-11-6 – User view of data (earth stations)

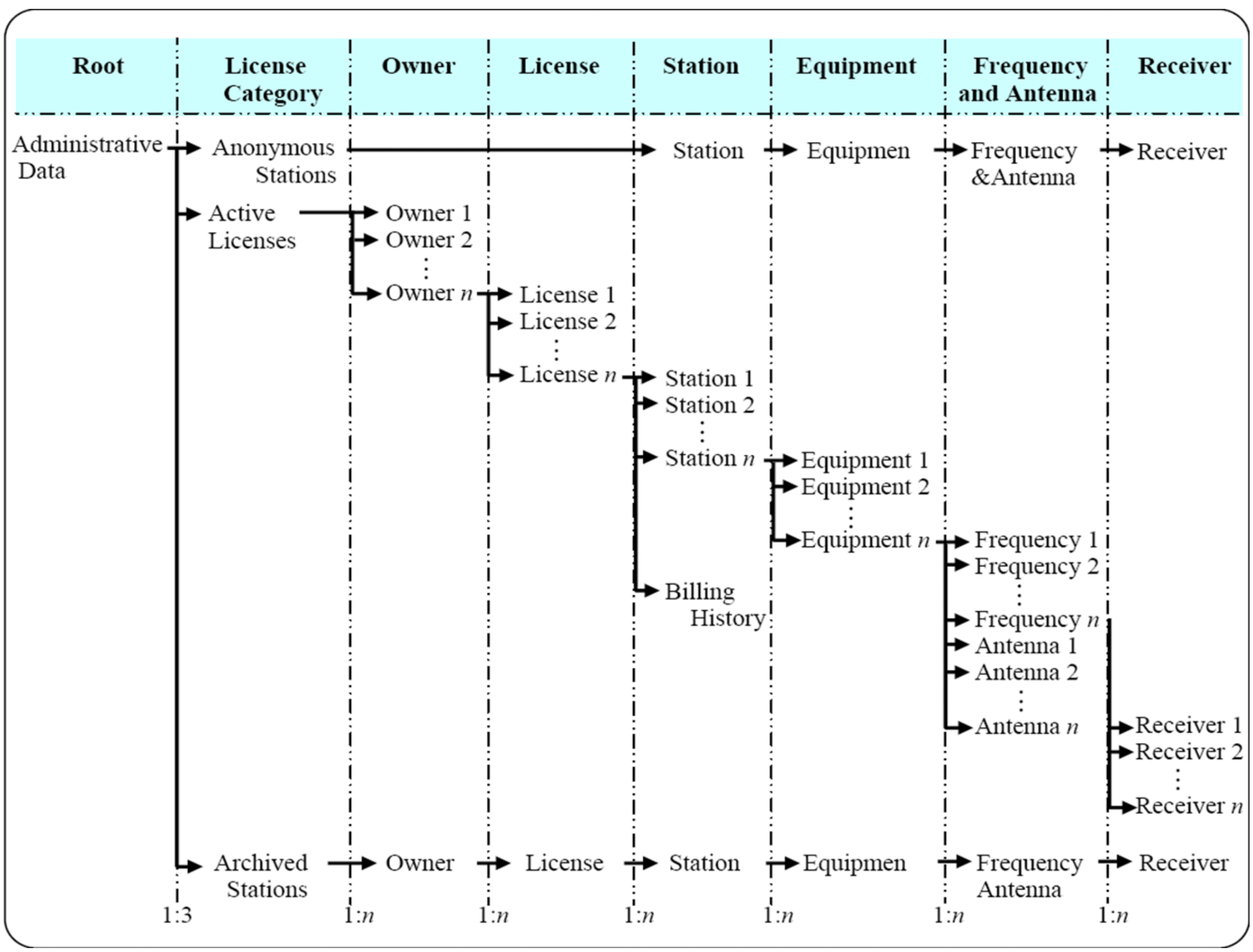



Figure 3-11-7 – Flow of administrative data entry

**References**

1. Martin Cave, Chris Doyle, William Webb, Modern Spectrum Management, Cambridge University Press, 2007 ISBN 0-521-87669-9
2. ITU-R, “Guidance on the regulatory framework for national spectrum management,” SM.2093-2, June 2015.
3. Bjorn Wellenius, Isabel Neto, “Managing the radio spectrum: framework for reform in developing countries,” the World Bank, March 2008.
4. ITU, “Spectrum management system for developing countries (SMS4DC) – Executive overview of the main features,” Available at http://www.itu.int/en/ITU-D/Technology/Documents/SpectrumManagement/SMS4DC_%20ExecutiveSummary_E.pdf
5. Resolution 9, “Participation of countries, particularly developing countries, in spectrum management,” ITU-D, June 2011.

# 4. Key Issues for broadband networks

## 4.1 Universal Access and Service

### 4.1.1. Overview

As the world becomes more dependent on ICT, broadband Internet access and usage is increasingly recognized as essential to economic growth and the provision of education, healthcare, and other basic services. Despite this growing acceptance, emerging countries continue to struggle to find affordable and sustainable ways to provide widespread access to digital devices and broadband connections, especially in rural and remote areas[83].

Universal access (UA) seeks to guarantee access to telecommunications infrastructure, sometimes on a shared basis, but does not necessarily concern itself with the availability of services, their affordability or accessibility. The concept is similar but different from that of universal service (US), which generally entails the availability of a basic set of communication services at an affordable price throughout a country. UA refers to a publicly shared level of service, e.g., through public payphones or Internet telecenters. US refers to service at the individual or household level, e.g., typically a telephone in each home. However, in more and more countries UA and US apply at the same time, and it therefore makes sense to use the generic term universal access and service (UAS). At a minimum, universal service guarantees a reliable access to a public telephone network at a fixed location that enables voice communication at an affordable price, free outgoing calls to emergency services[84].

In the past, developing countries typically focused primarily on UA as that was the appropriate and most feasible target. However, since the maturation of mobile communications, which extended services further and lowered access barriers to take up, many developing countries may now also realistically target US for telephony, at least in many urban areas. Over the past two decades, the scope of UAS has widened. Today, UAS is increasingly being re-conceptualized to include Internet – and even broadband – and to address issues around digital inclusion[85].

### 4.1.2. Technological, Economic and Policy Aspects

- **Technological Aspects**

Early developments in national UAS targeted public and private access to basic voice telephony services[86]. The rapid pace of technological innovation has a positive impact on the implementation of UAS. As UAS reached their potential and total universal service coverage became close to reality in many places, policy makers turned their focus towards affordable broadband access[87]. Thus, innovative technical solutions can be implemented at less cost provided that suitable technology is chosen based on the population's needs. However, UAS arrangements must remain technology-neutral, that is, they must not tilt the scales in favour of any given network when several are in competition on the services market. Transparency in the bidding process is another indispensable condition[88].

Mobile technology have all demonstrated their usefulness in extending access to rural areas. Infrastructure sharing and local roaming are two technical solutions that encourage the deployment of mobile networks.

- **Economic Aspects**

There are many approaches to public universal access financing. In most cases, the appropriate structure and set of partners depend on the type of project and its objectives. Three models could be considered for the UAS financing:

[83] ITU-D Question 7-3/1, "Implementation of universal access to broadband services," 2014

[84] Adapted from OECD WP on Communication Infrastructure and Service Policy, "Universal service policies in the context of national broadband plans," Jul. 2012

[85] ITU infoDev, Telecommunications Regulation handbook, 2011

[86] ITU, "Trends in universal access and service policies: changing policies to accommodate competition and convergence", 2009

[87] Adapted from Andrew Dymond, "Universal Service: The trends, opportunities and best practices for universal access to broadband services," Intelecon Research & Consultancy Ldt, 2010

[88] ITU-D Question 7-1/1, "Report on innovative solutions for the management and financing of universal service and universal access policies," 2006.

equity investment, public-private partnerships ("PPPs")[89] and financial incentives. The selection of a funding model will be based on criteria such as economic efficiency, transparency, cost effectiveness, etc[90].

The way in which UAS is organized and financed may have an effect on competition in the sector if it affects the viability of existing operators or the process whereby competitors enter the market. The way in which UAS obligations are allocated and financed therefore has a significant impact on the manner in which profits made in the telecommunication sector are shared among the different categories of consumer, businesses and even all tax payers. For these reasons the cost of providing universal access/service must be calculated before the financing system is implemented.

The deployment of broadband imposes several preconditions. In the past, this task came within the sole remit of the government, but today several countries have achieved their objectives by opening up the market to the private sector.

On the other hand, the affordability and accessibility of broadband services are largely determined by the prices that are charged for those services. Broadband suppliers need the flexibility to set and adjust their retail prices and price structures through trial and error[91].

- **Policy Aspects**

Universal access to broadband is a core concern for many countries. Its importance for ensuring universal service in remote areas is such that suitable policy is required to facilitate the inclusion of rural communities in the information and communication society.

The key goal of a country's UAS policy is to develop the infrastructure and regulatory tools necessary to provide each member of its population with access to a point of communication. Thus:

- Universal access relates to providing communities with affordable access to ICTs. Universal access policies work to increase access to telecommunications on a shared rather than individual basis, such as on a community or village level.
- Universal service is aimed at increasing the number of households with telecommunication services and providing telecommunication services to all households within a country, including those in rural, remote and high-cost locations. Universal service policies focus on ensuring that the cost of telephone services remains affordable to individual users or to targeted groups of users.

The ITU 2003 Trends in Telecommunication Reform Report articulates three main dimensions that characterize Universal Access and Universal Service:

- Availability: This relates to whether there is national coverage of ICT services (telephones and Internet). That is, the level of access to communication service is the same wherever a person lives or works, with no disadvantage stemming from geographic location.
- Affordability: National governments design policies and regulatory frameworks that include Universal Service Funds to address the challenges of network expansion. The goal is for everyone to be able to afford service, and no one is disadvantaged by income level.
- Accessibility: Persons with disabilities can use the service; one's level of physical and mental ability does not affect access to communication services. Policy makers must also take into account the relevance of content and applications and the ability of users to understand it[92].

### 4.1.3. Guidelines on the Implementation of Universal Access

These guidelines are presented by the Final Report of ITU-D Question 7-3/1 and are intended to achieve the implementation of universal access to broadband services:

- **Broadband National Strategies and Policies**

---

[89] See also ITU, Developing successful public-private partnerships to foster investment in universal broadband networks, 2013, http://itu.int/go/91OF

[90] ITU-D Question 7-3/1, "Implementation of universal access to broadband services," 2014

[91] ITU-D Question 12-3/1, "Tariff policies, tariff models and methods of determining the costs of services on national telecommunication networks, including next-generation networks," 2014

[92] ITU-D SG1 "Regulatory policy on universal access to broadband services," 2010

- Broadband UAS should be defined in consideration of minimum bandwidth.
- Various stakeholders should be involved in the telecommunication/ICT sector in order to reach a bilateral or multilateral cooperation to get to a good implementation of universal access to broadband services.
- Technological neutrality should always be taken into account in any envisaged solutions to face the problem of broadband access.
- Fair competition should be assured for promoting broadband access for all, and so on.

- **Financing Policies for Broadband UAS**
- Partnership cooperation between governments, operators and other various stakeholders to make available and affordable UAS and to ensure better coordination in the implementation of broadband UAS.
- Encourage cooperation in the establishment of networks and infrastructure as well as broadband services, to reduce costs and risks, through public-private sector partnerships.
- Fiscal measures to attract domestic and foreign investors could be envisaged in a transparent legal framework.
- Establishment of the Universal Service Fund (USF) programs for broadband and ICT.
- Ensure consistent management of the USF.

- **Programs for Broadband Deployment for Services and Applications**
- ICT/broadband programs that are funded by USF or by alternative mean can and should be sustainable. For that to occur, sustainability must be a key area of focus throughout the planning process.
- In applying USF in support of ICT/broadband programs countries are invited to shift policies to enable and support ICT-related programs and develop an overall national broadband plan.
- On broadband deployment, the countries should promote special package of broadband UAS to in respect of Agriculture, Education, Health, Governance etc.
- Sustainability is underpinned by targeted and comprehensive training and other educational programmes designed to ensure self-sufficiency in remote or underserved areas.

## 4.2 Emergency telecommunications

### 4.2.1. Overview[93]

In light of the recent natural and man-made disasters that have occurred, great attention and effort have been directed towards the application of radio communications for the purpose of disaster prediction, detection and mitigation. The ITU has developed recommendations that describe and define a telecommunication capability that will facilitate the use of public telecommunication services and systems by authorities for communications during emergency, disaster relief and mitigation operations.

During the World Telecommunication Development Conference (WTDC 14) Resolution 34 (Rev. Dubai, 2014), was approved on the role of telecommunications/information and communication technology (ICT) in disaster preparedness, early warning, rescue, mitigation, relief and response was unanimously approved by Member States. The same applied to Resolution 136 (Rev. Busan, 2014) of the ITU Plenipotentiary Conference in Busan, Korea, on the use of telecommunications/ICT technologies for monitoring and management in emergency and disaster situations for early warning, prevention, mitigation and relief was also approved by the conference. These two resolutions provide the mandate of ITU-D to focus on emergency telecommunication and the outcome was Object 5 output 2 which focuses on developing emergency telecommunication through workshops and in particular building the stock of emergency equipment that can be deployed to Member States when disasters strike.

The ITU has also started to the Smart Sustainable Development Model (SSDM)[94] initiative to create actions necessary to deploy the crucial telecommunications infrastructure that contribute to giving rapid assistance in case of natural disasters, and could also be used as a working tool to foster economic and social development, providing community telecommunication services where people can have access to education, health or best practices in any particular field.

- **Emergency situation and telecommunication**

(1) The nature of emergency situations

Disasters often happen as sudden events that cause immense damage, loss and destruction. Disaster events occur due to the forces of nature or because of actions that stem from human sources or interventions. Disasters can have extreme magnitude, be long lasting, and cover wide geographic areas within national or international boundaries. In other words, disasters are variable in magnitude (energy), duration (time), and geographic area. Regardless of the kind of disaster, telecommunications/ICTs are needed to respond effectively and save lives.

Since 2014, BDT has deployed emergency telecommunication equipment to more than 40 countries in the immediate aftermath of disasters. ITU have provided support for the deployment and for the airtime. The equipment included satellite phones, broadband terminals, deployable base station, and VSATs. Training on the use of the equipment was also provided to staff designated by government.

(2) Emergency response

All types of disasters, whether attributed to natural or human sources, can strike anywhere and anytime. Disaster recovery occurs in stages. The first responders to a disaster scene play the primary role in assessing and containing the damage. Other phases follow in quick succession. In the second phase the injured are treated and the saving of lives is priority. The third stage often brings additional disaster recovery personnel, equipment, and supplies, perhaps from pre-positioned sites, storage facilities or staging areas. The fourth phase comprises clean-up and restoration.

The common thread to facilitate operations for all disaster recovery phases is the utility of fast, reliable, user-friendly emergency telecommunications that may be realized by technical solutions and/or administrative policy.

(3) Assured telecommunications

---

[93] Relevant references on this topic are: ITU-T Y.1271 Framework(s) on network requirements and capabilities to support emergency telecommunications over evolving circuit switched and packet-switched networks, 2014; and ITU-T Y.2205 Next Generation Networks – Emergency telecommunications – Technical considerations, 2011.

[94] For more information on the ITU SSDM initiative see http://itu.int/go/LXI6

The goal is assured telecommunication capabilities during emergency situations. Disasters can impact telecommunications infrastructures themselves. Typical impacts may include: congestion overload and the need to re-deploy or extend telecommunications capabilities to new geographic areas not covered by existing infrastructures. Even when telecommunications infrastructures are not damaged by the disaster, demand for telecommunications soar during such events.

Circuit-switched networks respond to overload situations by denying call attempt when resources are saturated. One option is to pre-empt other callers when authorized emergency communication workers need to communicate. However, some types of networks respond to an additional load by degrading performance of the entire network. This occurs when networks operate under a best-effort framework where all information is treated the same and simply queued or dropped until network resources are available.

Providing a preferential treatment to emergency telecommunications and by providing fault tolerant networks that will not fail because any one component fails are important steps toward assured capabilities. While fault tolerant networks are a critical step toward assured capabilities, telecommunications network operators should also maintain recovery plans to restore networks in the event of failure.

- **Definitions: emergency telecommunication, emergency telecommunication service, telecommunication disaster relief and early warning**

It is essential that the different uses of these terms are agreed and understood. ITU-T Y.2205 defines them as follows:

- Emergency Telecommunication (ET): The umbrella term for any emergency-related service care that requires special handling from the NGN relative to other services.
- Emergency Telecommunication Service (ETS): A national service providing priority telecommunications to the ETS authorized users in times of disaster and emergencies [ITU-T E.107].
- Telecommunication Disaster Relief (TDR): The generic term for a telecommunications capability used for the purposes of disaster relief.
- Early Warning (EW): The generic term for all types of early warning systems, capabilities and services.
- Early warning system[95]: The set of capacities needed to generate and disseminate timely and meaningful warning information to enable individuals, communities and organizations threatened by a hazard to prepare and to act appropriately and in sufficient time to reduce the possibility of harm or loss.

This arrangement forms a tree with ET at the root for all activities. The use of terms and their inter-relationships is shown in Figure 4-2-1.

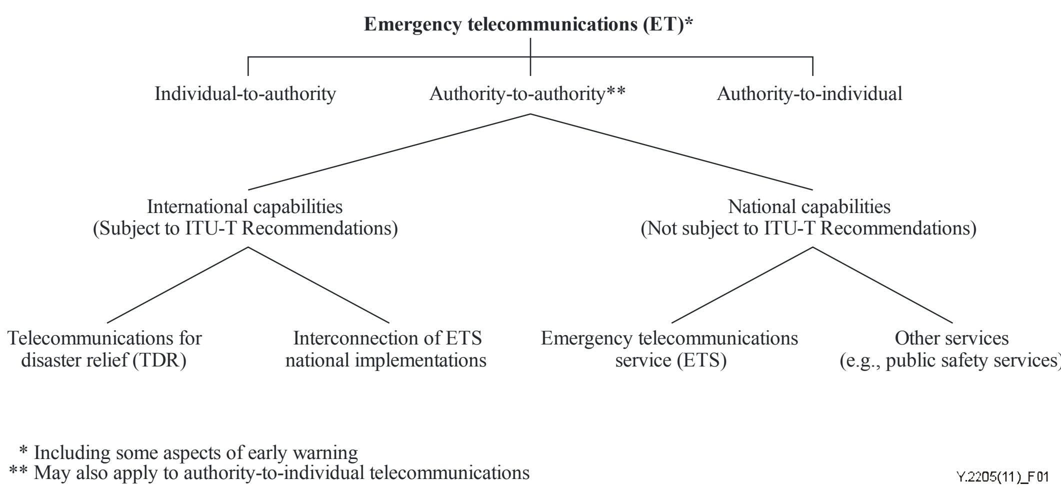



Figure 4-2-1. Terminological relationship framework for emergency telecommunications

(1) Emergency telecommunications

[95] Terminology used by the United Nations International Strategy for Disaster Reduction (UNISDR)

Emergency telecommunications (ET) means any emergency-related service that requires special handling from the NGN relative to other services. This includes government authorized emergency services and public safety services. The following are specific example services under the umbrella of emergency telecommunications:

- Telecommunications for disaster relief (TDR)

  TDR is an international and national telecommunications capability for the purpose of disaster relief. It can make use of international permanent, shared network facilities already in place and operational, temporary network facilities that are provisioned specifically for TDR, or a suitable combination of the two.

- Emergency telecommunications service (ETS)

  ETS is a national service, providing priority telecommunications to ETS authorized users in times of disaster and emergencies. The description of ETS is specified in [ITU-T E.107]. [ITU-T E.107] provides guidance that will enable telecommunications between one ETS national implementation (ENI) and other ENI(s) (authority-to-authority).

- National/Regional/Local emergency and public safety services

  Other examples of ET are national, regional, local emergency and public safety services. These are specialized services for national, regional, local emergencies and public safety. These emergency services are national, regional, or local specific and are subject to national or regional standardization.

(2) Early warning

The Sendai Framework for Disaster Risk Reduction is a guide for Member States on disaster-risk reduction. The framework was adopted during the Third World Conference on Disaster Risk Reduction, held in Sendai, Japan, from 14 to 18 March 2015. The Sendai Framework recognizes that Member States have the primary responsibility to prevent and reduce disaster risk, including cooperation. However, the Framework also recognizes that this is a shared responsibility between the central government and national authorities, private sectors, and stakeholders, as appropriate to national circumstances. The Sendai Framework places a great emphasis on disaster risk management efforts through an improved understanding of disaster risk in all its dimensions, and on the need to avoid the creation of new risks. The framework calls for the strengthening of international cooperation and global partnerships, and risk-informed donor policies and programmes. One of the goals is: Substantially increase the availability of and access to multi-hazard early warning systems and disaster risk information and assessments to the people by 2030[96].

- **Emergency Telecommunication Projects developed by ITU**

<u>Uganda Project</u>

A two-phased project was implemented and launched in Uganda. The project was for setting up a solar panel Early Warning System in Eastern Uganda, Butaleja District, an area which is vulnerable to floods and mudslides. Jointly with the Uganda Communications Commission, ITU launched the first phase of a red flood early warning system to warn residents on rising water levels. A second site was installed in December 2014 and completed on 5 January 2015. The project is based on the same principle as the one implemented by ITU in the Philippines, Catanduanes.

<u>Zambia Project</u>

A Cooperation agreement on setting up an early warning system was concluded between ITU and the Zambia Information and Communications Technology Authority (ZICTA) on 12 November 2014. The project is co-financed by both parties and. The project will be implemented at two pilot sites. The system will mainly be for the dissemination of alerts for flooding and mud sliding. The infrastructure will also be used for disaster preparedness and response.

.

[96] http://www.unisdr.org/we/coordinate/sendai-framework

Philippines project on Moveable and Deployable ICT Resource Unit (MDRU) in Philippines[97]

Typhoon Haiyan (Yolanda) the strongest recorded typhoon to make landfall devastated the Visayas region of the Philippines on November 8, 2013. The typhoon devastated much of the telecommunications network in the region for a significant amount of time, which slowed down the process of aid recovery and disaster management by local and national authorities

In this regard, ITU in cooperation with the Ministry of Internal Affairs and Communications (MIC), Japan will provide a Movable and Deployable ICT Resource Unit (MDRU) in the island of Cebu in the Philippines in order to study feasibility for restoring basic telecommunication infrastructure that was destroyed by typhoon Haiyan.

This project provides assistance to restore connectivity in one of the worst affected islands by typhoon Haiyan, by using the specific technology employed by MDRU, which was acknowledged by host countries as the preferable technology for responding to the aforementioned need.

### 4.2.2. Required Capabilities for Emergency Services[98]

- **General functional requirements and capabilities**

(1) Emergency telecommunications

The goal is to provide high confidence and probability that critical telecommunications will be available to perform reliably for authorized users, such as those involved in emergency telecommunications.

With respect to video and imagery, bandwidth (e.g., a form of resource) availability should be taken into consideration.

Emergency telecommunications specific network functions can be divided into the following categories: service invocation, authentication and authorization, end-to-end priority treatment, network interconnection and protocol interworking.

A service invocation pertains to user interaction with the user element (e.g., telephone) and the network with information that indicates an emergency telecommunications service request to the service provider network. There are different approaches including subscription arrangements for recognizing the request. Subscription information is used to authorize some service requests.

Authentication and authorization is performed by the service provider to allow or deny the user access to the invoked service for emergency telecommunications. The authorization itself is expected to occur at the core network.

End-to-end priority treatment is a set of capabilities used by the network(s) in providing high probability in establishing and maintaining the service from the originating network to the terminating network including any transit networks. The priority treatment persists with the service invocation to release of the service. The priority treatment is included in admission control and allocation of network resources, and transport of signalling and media bearer packets by the network elements supporting the service.

Network interconnection and protocol interworking is necessary for supporting end-to-end priority treatment for signalling and media transport traversing multiple networks belonging to different providers using different technologies. As an example, the levels of priority may vary depending on the technology used in the multiple networks and mapping from a level defined in one technology to another may be required.

(2) Early warning

Early warning systems need an effective communication system that is reliable and robust. Some objectives for early warning systems in the context of the NGN as the communication system are to:

- have continuously operating capabilities and be operational, robust, available every minute of every day;
- provide the needed telecommunication capabilities to transmit real-time (e.g., seismic and sea-level data information);
- be based on internationally agreed standards;

[97] For more information about this project: http://www.itu.int/net4/ITU-D/CDS/projects/display.asp?ProjectNo=9PHI14003

[98] ITU-T Y.1271 (Framework(s) on network requirements and capabilities to support emergency telecommunications over evolving circuit switched and packet-switched networks), ITU-T Y.2205 (Next Generation Networks – Emergency telecommunications – Technical considerations)

- ensure the integrity of early warning systems and the integrity and authenticity of messages (i.e., that only authorized messages are sent);
- provide warning messages only to those possibly affected by an impending disaster and prevent untargeted and unnecessary messages. (e.g., messages sent to the wrong people and/or messages that do not contain useful viable information).

In order to provide warning messages only to those possibly affected by an impending disaster, early warning systems may have objectives related to the filtering of messages so that these reach a selected:

- group of users;
- region or geographical area, etc.

- **General security guidelines and requirements**

(1) General guidelines

The network elements, systems, resources, data, and services used to support emergency telecommunications can be targeted for cyber attacks. The integrity, confidentiality, and availability of emergency telecommunications, especially when under attack, will depend on the security services and practices implemented in the NGN and on the security capabilities (e.g., user authentication and authorization functions) implemented as part of the application service for emergency telecommunications. General guidelines to consider for emergency telecommunications security planning include (but are not limited to):

- All aspects of emergency telecommunications including the signalling and control, bearer/media, and management-related data and information (e.g., user profile information) need to be protected against security threats. Security threats to emergency telecommunications could occur at various layers (e.g., transport, service control or service support) and in the different network segments (i.e., access, core network, and interconnection interfaces).
- Establishment and enforcement of security policies and practices that are specific to emergency telecommunications services. Mitigation capabilities to provide protection against various security threats should be identified and implemented.
- Implementation and use of procedures to authenticate and authorize users, devices or the combination of user and device to protect against unauthorized access to services, resources and information (e.g., user information in authentication servers and management systems) associated with emergency telecommunications.
- Responsibility within each network for security within its domain for communications that traverse multiple network provider domains so that the end-to-end communication can be secured. Since emergency telecommunications may involve communications that traverse different network provider domains of national and international networks (i.e., countries and administrations), security policy, trust relations, methods and procedures for identifying emergency telecommunications traffic, identity management and authentication of users and networks across multiple network administration domains need to be established and implemented.

(2) General requirements

The security recommendations in [ITU-T Y.2701], [ITU-T Y.2702], and [ITU-T Y.2704], and the identity management (IdM) recommendations in [ITU-T Y.2720], [ITU-T Y.2721], and [ITU-T Y.2722] are relevant to emergency telecommunications security.

- Access control

  Only authorized users must be allowed access to emergency telecommunications and any associated resources. Any unauthorized access, such as that by intruders masquerading as authorized users, must be prevented.

- Authentication

Mechanisms and capabilities to identify, authenticate and authorize access of the emergency telecommunications user, device or user and device combination as applicable based on policy[99] and the assurance level for specific service (e.g., voice, data, video) is necessary for security protection.

- Confidentiality and privacy

  Confidentiality and privacy protection of emergency telecommunications and end-user information are necessary. This includes confidentiality and privacy protection of emergency telecommunications signalling, control and bearer traffic, end-user information (e.g., identity, subscription and location information) and activity, as applicable.

- Communication security

  Protection of emergency telecommunications against intrusions is necessary (e.g., prevention of unlawful interception, hijacking or replay of signalling or bearer traffic).

- Data integrity

  Integrity protection of emergency telecommunications is necessary (e.g., protection against unauthorized modification, deletion, creation, or replay). This includes integrity protection of emergency telecommunications information and any configuration data (e.g., priority marking, priority information stored in policy decision functions, user priority level, etc.).

- Availability

  Availability of emergency telecommunications must be protected. Specifically, emergency telecommunications and any associated resources must be protected against denial of service (DoS) and other forms of attacks.

- **Emergency telecommunications requirements and capabilities**

Fully comprehensive emergency telecommunications need to have many capabilities to support a variety of operational requirements for emergency recovery forces.

- Enhanced priority treatment

  Telecommunication network operators and service providers (SP) need to be able to identify and prioritize emergency telecommunications according to their SLA with users. New or temporary emergency operations users require a network operator to provision an access line. It is desirable for provisioning to occur on a preferential basis to enable rapid initiation of emergency communications.

- Secure networks

  Security protection is necessary to prevent unauthorized users from obtaining scarce telecommunication resources needed to support emergency operations.

- Location confidentiality

  Emergency telecommunications from selected users need to be protected from manipulation, interception or obstruction by others, due to their urgent and important nature. Special security mechanisms to prevent the identification of the location of certain authorized users of emergency telecommunications from being revealed to non-authorized parties should apply in order to protect such authorized users from being located.

- Restorability

  Both circuit- and packet-switched networks typically require a physical access line, wired or wireless, that extends to customer locations. When access lines are damaged, network operators restore operations but access disruption times may be lengthy. Therefore, it is necessary for restoration to occur on a preferential basis to enable rapid initiation of emergency telecommunications for users of these capabilities.

---

[99] Policy in this context includes all applicable policies such as those generated from NGN provider decisions, regulatory requirements, or other governmental rules.

- Network connectivity

  It is advisable that networks supporting emergency telecommunications be connected to other networks thereby providing a wide reach. Interworking preferential treatment at reference points that are deemed to constitute international and/or regulatory boundaries between national networks that provide emergency telecommunications may create international emergency systems, e.g., when ITU-T Rec. E.106 is applicable.

- Interoperability

  Evolving networks will produce a number of issues, one of which is to ensure orderly and transparent continuance of the basic ITU-T Rec. E.106 emergency preference capabilities. During the convergence period, the different schemes for interworking between the circuit-switched and packet-switched technologies need to be considered.

- Mobility

  In order to have mobile capabilities, a common configuration provides key elements to facilitate capabilities for emergency applications. The telecommunications infrastructure should support user and terminal mobility including re-deployable, or fully mobile telecommunications.

- Ubiquitous coverage

  Public telecommunication infrastructure resources over large geographic areas should form the framework for ubiquitous coverage of emergency communications.

- Survivability/endurability

  Capabilities should be robust to support surviving users under a broad range of circumstances, from the widespread damage of a natural or human-made disaster.

- Voice transmission

  Networks need voice transmission capabilities for emergency operations. Circuit-switched networks provide this by default while packet-switched networks require support of: low jitter, low loss and low delay for acceptable interactive real time voice media streams. Circuit-switched and packet-switched networks need to provide voice transmission quality service for emergency telecommunications users.

- Scalable bandwidth

  Broadband is a user requirement that may be requested during acquisitions of emergency telecommunications from operators. Authorized users should be able to select the capabilities of emergency telecommunications to support variable bandwidth requirements.

- Reliability/availability

  To provide the greatest utility, emergency telecommunications need to be both reliable and available. Whenever possible, admission control or network policy can increase the probability of successful telecommunications by providing a preferential treatment to emergency telecommunications.

  Telecommunications should perform consistently and precisely according to their design requirements and specifications, and should be usable with high confidence.

- **Risk analysis service**

Risk analysis service is a service that is capable of identifying risks, assessing them and then invoking processes to identify the proper actions that should be taken to reduce damage that could affect users or organizations subscribed to a next generation network (NGN)[100].

Provided that a risk situation exists, the risk analysis function performs the analysis and assessment of the risk event data with an algorithm that applies the most recent pattern according to procedures, and reports the analysis results and the proper complementary measures which, if invoked, will reduce risk.

---

[100] ITU-T Supplement 19 on the risk analysis service in next generation networks, 2012.

The risk analysis service (IRAS) must contend with internal risks, which are risks related to potential network providers, service providers and user/terminal failures, as well as with external risks, which are risks related to forces external to the network.

Figure 4-2-2 shows a conceptual model for an IRAS function.

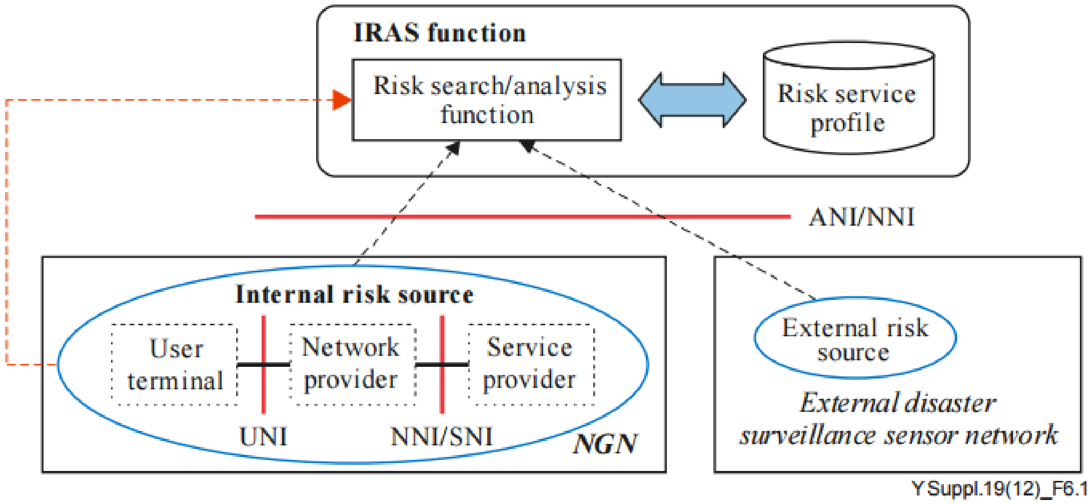



Figure 4.2.2 – Conceptual models for IRAS

### 4.2.3. Technical solutions for Emergency Services[101]

- **Mechanisms and capabilities supporting emergency telecommunications in NGN**

In an NGN where the service and transport stratum are independent, the following factors influence the success of an emergency telecommunication:

- identification and marking of the emergency telecommunication traffic;
- admission control policy;
- bandwidth allocation policy;
- authentication and authorization of bona fide emergency telecommunications users.

(1) Service stratum

Countries have, or are developing, ETS to allow priority treatment for authorized traffic to support emergency and disaster relief operations within their national boundaries. However, there could be a crisis situation where it is important for an ETS user in one country to communicate with users in another country. In this case, it is important for an ETS call or session which originated in one country to receive end-to-end priority treatment, i.e., priority treatment in the originating country and the destination country. This may require interconnection of two ETS national implementations via an international network that either provides priority treatment capabilities, or convey the priority transparently between both countries.

(2) Transport stratum

The need for special arrangements (e.g., Service Level Agreement (SLA)) to handle ET in a properly-engineered and dimensioned NGN is based on an assumption that the network resources are inadequate for the amount of traffic being offered to the network, and that under such conditions emergency telecommunications traffic could be rejected or significantly delayed and/or disrupted beyond the point of being usable, or even be discarded.

(3) NGN access technology support

To support emergency telecommunications, special arrangements are also needed in the NGN access segment. The need for special arrangements is based on the assumption that in the same way that the core network resources are

[101] ITU-T Y.2205 Next Generation Networks – Emergency telecommunications – Technical considerations, and ITU-D Q 22/2 Guidelines on the Common Alerting Protocol (CAP), 2009.

limited, access resources are also limited. Therefore, depending on the amount of traffic being offered to the access network segment, emergency telecommunications traffic could be impacted (e.g., rejected or significantly delayed and/or disrupted beyond the point of being usable, or even be discarded).

Therefore, if the NGN is to be capable of handling all kinds of emergencies under adverse circumstances, the availability of specific means to provide preferential treatment of emergency telecommunications traffic needs to be supported in the NGN access segment. This includes, but is not limited to, mechanisms and capabilities for:

- recognizing emergency telecommunications traffic;
- preferential/priority access to resources/facilities;
- preferential/priority routing of emergency telecommunications traffic;
- preferential/priority establishment of emergency telecommunications sessions/calls.

In establishing priority treatment for emergency telecommunications, the following aspects are considered: classifying or labelling the traffic for priority treatment, signalling to set up the path for transporting this traffic and mechanisms including the policies to support the requested priority. Some aspects such as the selection of mechanisms, policies and associated implementations are not standardized and may be region specific.

- **End-to-end support for emergency telecommunications**

Figure 4-2-2 shows an end-to-end call or session matrix for supporting various ETS call or session flows. It illustrates calls or sessions:

- originating and terminating on IP (e.g., Cable and DSL), narrow-band wireline (e.g., POTS phone), and wireless (e.g., GSM and CDMA phone) access; and
- traversing through IP and circuit-switched (TDM) core networks.

Support of the end-to-end ETS requires the interworking of ETS specific information between the IP technology domain and other technology domains (e.g., wireless or wireline TDM domains). This includes the necessary interworking for the end-to-end ETS call or session that may cross different technology domains shown in Figure 4-2-3. For example, the ETS specific information (e.g., ETS call marking, priority level) needs to be signalled across the network-to-network interface (NNI) between interconnecting NGN providers.

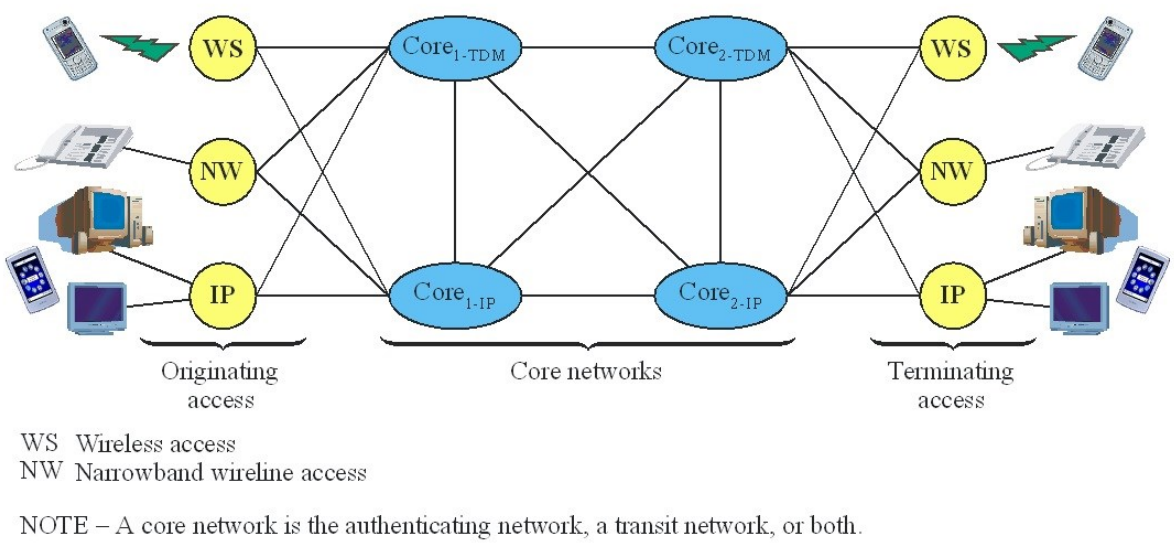



Figure 4-2-3. End-to-end call or session matrix

Setting up the ETS call or session requires careful implementation of the necessary signalling protocols that convey the required information signifying the critical nature of ETS. In order to support end-to-end priority treatment, it is important to support the mapping of priority information to facilitate seamless protocol interworking between the different protocols used within a network (e.g., vertical protocol interworking between call or session control and bearer control) or between different network types (e.g., call or session control interworking between two networks) including PSTN. Similarly, it is critical to allow mapping of priority information to facilitate seamless interworking between the different transport types, i.e., media types. Without such an interworking/mapping, end-to-end priority treatment may not be achievable.

- **Mechanisms and capabilities supporting some aspects of early warning in NGN**

(1) General

Alert systems used for early warning may be classified by whether they employ a push or pull models.

The push model relies on participants registering their contact information (e.g., an e-mail address) to a central service. When an event occurs, these registered participants are alerted to the event with potentially more pointers to additional information. A key architectural design in this model is that a central authority determines if information is to be disseminated, and what that information entails. The strength in this model is that it takes on the burden of being active in monitoring events, thus allowing users to continue in their normal responsibilities and remain passive concerning the monitoring of potential disasters or emergencies.

The pull model is the opposite of the push model in that the former relies on a query-response exchange of information. While both models rely on registrations by individual participants, the pull model places the responsibility of monitoring and obtaining information onto the individual users. The advantage of this system is that information is only provided on an as-needed or on-demand basis.

(2) Common alerting protocol (CAP)[102]

The common alerting protocol (CAP) allows a consistent warning message to be disseminated simultaneously over many different warning systems, thus increasing warning effectiveness while simplifying the warning task. CAP also facilitates the detection of emerging patterns in local warnings of various kinds, such as might indicate an undetected hazard or hostile act. CAP also provides a template for effective warning messages based on best practices identified in academic research and real-world experience.

The CAP provides an open, non-proprietary message format for all types of alerts and notifications. It does not address any particular application or telecommunications method. The CAP format is compatible with emerging techniques, such as web services and the ITU-T fast web services, as well as existing formats including the specific area message encoding (SAME) used for the United States National Oceanic and Atmospheric Administration (NOAA) weather radio and the emergency alert system (EAS), while offering enhanced capabilities that include:

- flexible geographic targeting using latitude/longitude shapes and other geospatial representations in three dimensions;
- multilingual and multi-audience messaging;
- phased and delayed effective times and expirations;
- enhanced message update and cancellation features;
- template support for framing complete and effective warning messages;
- compatibility with digital encryption and signature capability; and
- the facility to transmit digital images and audio.

CAP provides reduction of costs and operational complexity by eliminating the need for multiple custom software interfaces to the many warning sources and dissemination systems involved in all-hazard warning. The CAP message format can be converted to and from the "native" formats of all kinds of sensor and alerting technologies, forming a basis for a technology-independent national and international "warning internet".

(3) Service restoration priority

In the event of a network failure or outage, critical services (e.g., emergency services) can be interrupted and may need a higher probability of successful restoration over other services. [ITU-T Y.2172] specifies three levels for restoration priority for services in NGN. It allows for such priority classifications to be used in signalling messages such that the service in question can get call or session set-up with the desired restoration priority, thus allowing critical services to have a higher probability of successful restoration over other services.

(4) Protection switching and restoration

[102] ITU-T X.1303 (09/2007); and ITU-T X.1303 bis Common alerting protocol (CAP 1.2), 2014

A number of general concepts common to many transport technologies are described in [ITU-T G.808.1]. Several important issues to be considered when providing protection for emergency telecommunications traffic are identified in [ITU-T G.808.1].

- Individual protection

  The individual protection concept applies to those situations where it is useful to protect only a part of the traffic signals which need high reliability.

- Group protection

  This allows protection switching through the treatment of a logical bundle of transport entities as a single entity after the commencement of protection actions.

- Architectural types

  The following architecture types are identified in [ITU-T G.808.1] and are summarized below.

  – 1+1 protection architecture: In the 1+1 architecture type, a protection transport entity is dedicated as a backup facility to the working transport entity.
  – 1:n protection architecture: In the 1:n architecture type, a dedicated protection transport entity is a shared backup facility for n working transport entities.
  – m:n protection architecture: In the m:n architecture type, m dedicated protection transport entities share backup facilities for n working transport entities, where $m \leq n$ typically.

- Switching types

  The protection switching types can be a unidirectional switching type or a bidirectional switching type.

  It should be noted that all switching types, except 1+1 unidirectional switching, require a communications channel between the two ends of the protected domain; this is called the automatic protection switching (APS) channel.

  In the context of an IP-based emergency telecommunications, unidirectional switching may be adequate since, in general, the paths in each direction are not directly associated due to the nature of unidirectional nature of paths/routing through IP-based networks.

- Operation types

  The protection operation types can be a non-revertive operation type or a revertive operation type.

  In revertive operation, the traffic signal (service) always returns to (or remains on) the working transport entity when it has recovered from the defect.

  In non-revertive operation, the traffic signal (service) does not return to the original working transport entity.

(5) Suggestions for immediate actions to implement the Common Alerting Protocol (CAP) content standard

- Policy-makers, regulators and telecommunication operators

  Explore policy actions that serve to promote the all-hazards, all-media approach to public warning, and specifically the dissemination of public alert messages in CAP format. In most cases, the immediate challenge will be to educate key organizations and agencies as to the potential of this approach, not only from a public policy perspective but from a market opportunity perspective as well. It may also be useful to form multiparty working groups at a regional level to coordinate among stakeholders.

- Sources of public warnings

  Within existing policy mandates, implement dissemination of public alert messages in CAP format, typically on the public Internet and with a Rich Site Summary (RSS) news feed. Of course, other approaches may be needed for rapid dissemination of time-critical alerts, and each CAP implementation should supplement current dissemination methods of alerts. Provision of CAP alerts may be offered directly by the alerting source, or through intermediaries. In any case, subscriber access to the CAP alerts should include one of the common mechanisms to assure authenticated delivery and evidence of authority. It is important that sources are quite clear as to the extent of authority for issuing alerts to particular localities.

- Receivers of public warnings

  Within existing policy mandates, implement procedures to receive public alert messages in CAP format. The implementation should supplement current dissemination methods, and should make use of the common mechanisms to assure authenticated delivery and evidence of authority.

- Intermediaries for public warnings

  Add features and develop products and services that handle CAP alert messages, with mechanisms for authenticated delivery and automated processing. Network service and product providers may provide filtering and routing services or products that transmit public alert messages in CAP format from authoritative public alerting sources or authoritative retransmission agents.

- Other infrastructure components for public warning

  Authorization and authentication service providers may develop products and services that provide mechanisms for end-to-end assurance of authenticity and evidence of authority, validated for handling of alert messages in CAP format during emergency situations. ICT hardware, software and services vendors may add features that handle CAP alert messages, with mechanisms for authenticated delivery and automated processing where appropriate. ICT devices and software could feature geographic display of emergency information by targeted area using streams of alert messages in CAP format.

- Other actors in disaster management

  The immediate challenge is to educate these other actors about the emergence of a standards-based, all-media, all-hazards public warning infrastructure on the national, regional, and global scales. There are many opportunities to leverage the warning infrastructure for commercial gain as well as for the public good.

### 4.2.4. Disaster Relief Systems, Network Resilience and Recovery[103]

- **Overview of Disaster Relief Systems, Network Resilience and Recovery (DR&NRR)**

DR&NRR are designed to provide users with telecommunication services to protect their lives and assets when there is a disaster that may significantly destroy network infrastructures and disrupt connectivity. The study area of DR&NRR is very broad and so some study items are classified according to the particular phases of a disaster as shown in Figure 4-2-4, which can be categorized as "before disaster", "at and during disaster" and "after disaster".

[103] ITU-T Focus Group on Disaster Relief Systems, Network Resilience and Recovery (FG-DR&NRR) Deliverables, ITU-T Focus Group on Smart Sustainable Cities Deliverables.

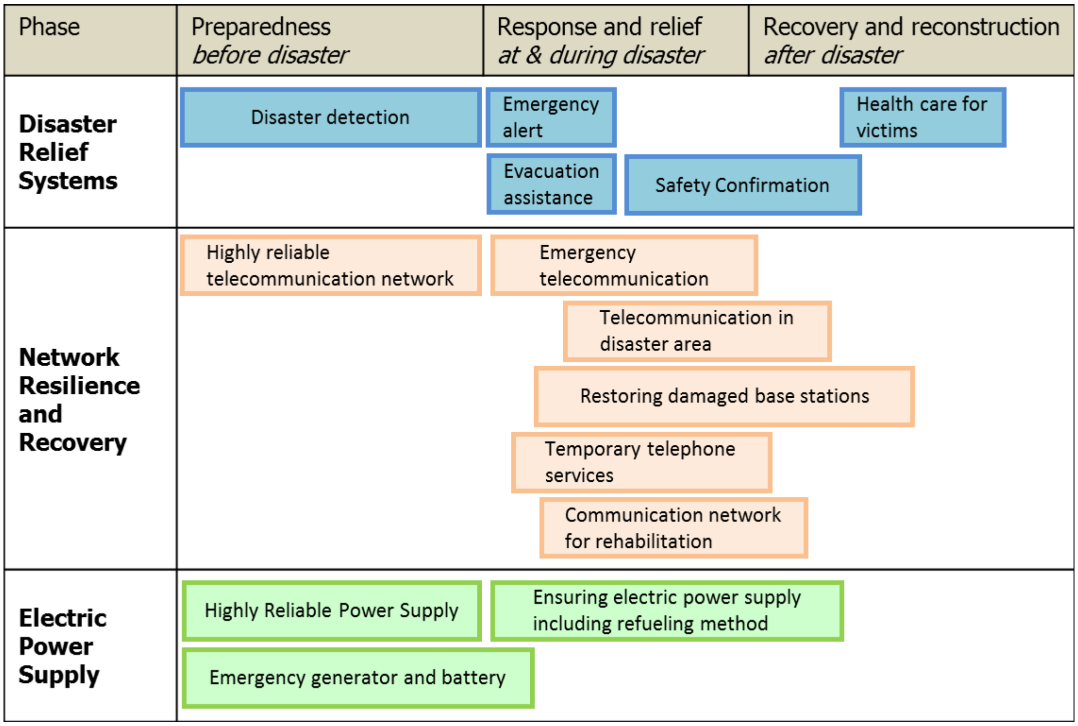


Figure 4-2-4. Overview of expected study areas for DR&NRR

- Disaster relief systems

A disaster detection and early warning system is required so that we are prepared before a disaster occurs. During an incident or a disaster, an emergency alert system and an evacuation assistance system are used to evacuate people from potentially dangerous areas and rescue those in danger. A safety confirmation system is utilized to confirm the safety of each person and assist rescue work immediately after an incident and for a certain period of time during a disaster. A system supporting health care and for sustaining the lives of the victims may also be necessary for a relatively long time after an incident.

- Network resilience and recovery

Network resilience and recovery depends on a highly reliable network design, such as a multiple network route. For emergency telecommunications it is useful to establish temporary telephone services by temporarily restoring damaged mobile base stations after a disaster.

In addition to the scenarios (or use cases) involving the of strengthening existing networks in operation, it is necessary to consider a complementary approach that mobilizes ICT facilities surviving in the devastated area, connects them with instantly deployable and configurable ICT resources, and then builds local networks to satisfy the urgent need for local communication between rescue teams and local citizens in the area.

- Electric power supply

A highly reliable way of guaranteeing an electrical power supply for telecommunication equipment must be ensured by using, for example, multiple electrical distribution routes and an electrical generation system. An effective way of refuelling electrical power generators after a disaster should be considered.

- **Requirements for DR&NRR**

- Disaster relief systems

During and after disasters disaster relief systems provide people with timely and useful information that is used for rescue, evacuation, safety confirmation and even to sustain life. Regarding the service and application aspect, systems that provide early warning against imminent disasters help people prepare for them, prevent serious damage, minimize the damage if it cannot be prevented, and reduce the loss of human life to the bare minimum.

The response of people affected by a disaster is to attempt to call to report that they are safe or to call to check whether others are safe, causing telecommunications network congestion. It is therefore necessary to implement measures to alleviate congestion. Congestion can be avoided by:

– encouraging alternative means of communication,
– reducing call hold times,
– reducing call quality,
– reassigning network resources to telephony, or
– developing new network architectures that can handle spikes in telephone traffic.

Priority can also be given to users with special privileges to make calls during disaster situations. Services for emergency and disaster related organizations are also given high priority.

- Telecommunication network resilience and recovery

NRR denotes the following capabilities of telecommunication networks and related processes to cope with disasters:

– Resilience: the ability to provide and maintain an acceptable level of services in the face of faults and challenges to the normal operation of a given communication network, based on prepared facilities
– Recovery: the process of restoring the normal level of service of a given communication network after a disaster, possibly with the deployment of additional available facilities

Based on an analysis of use cases, the following general requirements for NRR have been identified (the list is not all-embracing).

– redundancy in facilities
– facility placement at secure locations
– effective use of radio communications
– inter-operation of heterogeneous networks
– availability of quickly deployable facilities
– congestion mitigation

It is clear that locating equipment where it is least exposed to risk can reduce infrastructure damage. The use of aerial facilities should be avoided and critical equipment such as authentication servers should be geographically dispersed.

- Electric power supply

It is clear that locating equipment where it is least exposed to risk can reduce infrastructure damage. A steady power supply and power generation equipment should be located at a place where it is least exposed to potential damage from a disaster.

Disasters related to water, including flooding and tsunami, may cause significant damage to power supply systems. The equipment should be installed at a higher location on land or in a building where the risk of flooding is reduced. The use of multiple electrical distribution routes is recommended and aerial facilities should be avoided.

An autonomous power supply is critical and there should be sufficient fuel for back-up generators as power outages can be lengthy. Equipment should be installed in buildings in higher locations where the risk of flooding is reduced and basements should be avoided as sites for equipment and reserve generators. Spare power supplies, back-up generators, or batteries should be prepared to ensure a stable power supply and thus maintain continuous communication services when the main power fails. The autonomous power supply should be capable of lasting at least 72 hours to allow time for sufficient and effective rescue work.

- **Emergency/Disaster Response Mechanisms in Smart Cities**

During a disaster or emergency, a smart city must maintain operations required to address time-sensitive, disaster-specific issues. No plan can anticipate or include procedures to address all the human, operational and regulatory issues. Essential business transactions must function, addressing needs assessment, communication, volunteer outreach and coordination, grant applications, and community assistance under rapidly changing circumstances.

A smart city should have carried out risk assessment with respect to its susceptibility to various natural disasters and should have strategy in place to deal with natural disaster to which it is highly susceptible.

A smart city's disaster resilience solutions should cover observation systems, information gathering capabilities, data analysis and decision making aids. These components matched with an intelligent and interoperable warning system will enable cities to respond effectively to natural disasters. This heavily depends on the municipality's uses of ICT infrastructure, including mobile networks, to efficiently receive, process, analyse and re-distribute data, and mobilize various city services.

During the Disaster Prevention phase, the use of ICTs such as Geographic Information Systems (GIS) in local hazard mapping and analysis can help to identify and illustrate evacuation routes as well as to locate housing, business and structures that are at risk of threats such as rises in water levels.

When a disaster occurs and emergency takes place, technical standards facilitate the use of public telecommunication services and systems for communications during emergency and disaster relief operations. This capability, referred to as the emergency telecommunication service, enables authorized users to organize and coordinate disaster relief operations as well as have preferential treatment for their communications via public telecommunication networks. This preferential treatment is essential as public telecommunication networks often sustain infrastructure damage which, coupled with high traffic demands, tends to result in severe congestion or overload to the system. In such circumstances, technical features need to be in place to ensure that users who must communicate at a time of disaster have the communication channels they need, with appropriate security and with the best possible quality of service.

To ensure reliable universal access to communication in extreme weather event, the CAP developed by ITU provides a general format for exchanging all-hazard emergency alerts and public warnings over all kinds of networks. CAP allows a consistent warning message to be disseminated simultaneously over many different warning systems, thus increasing warning effectiveness while simplifying the warning task.

#### 4.2.5. Standardization for Emergency Services and other initiatives

- **ITU-D Activities**

  ITU-D Study Group 2 has published "Utilization of ICT for disaster management, resources, and active and passive space-based sensing systems as they apply to disaster and emergency relief situations" as a result of Question 22/2. The document provides some guidelines regarding the CAP.

  ITU-D SG 2 has developed the ITU Handbook "Telecommunication outside plants in areas frequently exposed to natural disasters" and "Emergency Telecommunications".

  ITU-D Study Group question 5/2[104] deals with the utilization of telecommunications/ICTs for disaster preparedness, mitigation and response.

- **ITU-T activities[105]**

  Various ITU-T study groups are undertaking advanced work on emergency telecommunications. As the lead study group on this theme, ITU-T Study Group 2 is continuing to develop Recommendations for Telecommunication for Disaster Relief/Early Warning. Other Study Groups have developed Recommendations for communications in emergency situations and for a telecommunication network that remains highly reliable in a disaster. There are some standardization activities in the study areas of safety confirmation, health care for victims, temporary telephone services and power supply issues before/during a disaster.

  - Actvities under ITU-T SG15:

[104] http://www.itu.int/en/ITU-D/Emergency-Telecommunications/Pages/sg_question_et.aspx.

[105] ITU-T Focus Group on Disaster Relief Systems, Network Resilience and Recovery (FG-DR&NRR) Deliverables.

The following two Recommendations based on the deliverables from the ITU-T Focus Group on Disaster Relief Systems, Network Resilience and Recovery (FG-DR&NRR) are ongoing:

- ITU-T L.nrr-frm: "Framework of disaster management for network resilience and recovery" [106]
- ITU-T L.dm-nrr-mdru :"Disaster management for improving network resilience and recovery with movable and deployable ICT resource units"[107]

- Activities under ITU-T SG2:

Recommendation ITU-T E.108 "Requirements for a disaster relief mobile message service" was approved in its last meeting of January 2016.

Based on the deliverables from the ITU-T Focus Group on Disaster Relief Systems, Network Resilience and Recovery (FG-DR&NRR), three work items are under development in ITU-T SG2:

- A new work item on draft new ITU-T E.rdr-scbm "Requirements for Safety Confirmation and Broadcast Message Service for Disaster Relief" was agreed in the last SG2 meeting.[108]
- The following two work items are on-going in SG2:
  - o Draft new ITU-T E.TD-DR "Terms and definitions for DR&NRR"[109]
  - o Draft new ITU-T E.RDR "Requirements for Disaster Relief Systems"[110]

- **ITU-R**

Aspects of radio communication services associated with disasters include disaster prediction, detection, alerting and relief. In certain cases, when the "wired" telecommunication infrastructure is significantly or completely destroyed by a disaster, only radio communication services can be employed for disaster relief operations. The relevant ITU-R activities may be categorized into the following 5 study items: Disaster prediction and detection, Emergency alert, Evacuation assistance, Telecommunication in disaster area, Highly reliable telecommunication.

- **ITU/WMO/UNESCO IOC Joint Task Force on Green Cable[111]**

ITU, together with the Intergovernmental Oceanographic Commission of the United Nations Educational, Scientific and Cultural Organization (UNESCO/IOC) and the World Meteorological Organization (WMO), established the Joint Task Force (JTF) in late 2012 to investigate the use of submarine telecommunications cables for ocean and climate monitoring and disaster warning. The JTF 2014 Annual Report can be access on line[112].

- **International Organization for Standardization (ISO)/ International Electrotechnical Commission (IEC)**

---

106 latest draft: TD195Rev.1 (WP2/15) http://www.itu.int/md/T13-SG15-150622-TD-WP2-0195/en

107 latest draft: TD196Rev.1 (WP2/15) http://www.itu.int/md/T13-SG15-150622-TD-WP2-0196/en

108 draft new ITU-T E.rdr-scbm "Requirements for Safety Confirmation and Broadcast Message Service for Disaster Relief"

109 Draft new ITU-T E.TD-DR "Terms and definitions for DR&NRR"

110 Draft new ITU-T E.RDR "Requirements for Disaster Relief Systems"

111 Details and publications are available at: http://itu.int/en/ITU-T/climatechange/task-force-sc.

112 http://www.itu.int/en/ITU-T/climatechange/task-force-sc/Documents/JTF_2014_Annual_Report.pdf

A highly reliable power supply and electric power distribution technology are being discussed by IEC technical committee 96 (Transformers, reactors, power supply units, and combinations thereof).

- **Internet Engineering Task Force (IETF)**

The Internet Engineering Steering Group (IESG) established an IETF Working Group (WG) in the Real Time Applications and Infrastructure Area) to address Internet Emergency Preparedness (IEPREP). Some informational RFCs in two specific technical areas were developed: “Requirements for Internet Emergency Preparedness in the Internet”, and the “Framework for Supporting Internet Emergency Preparedness in IP Telephony.”

Table 1 presents a list of publication on Emergency Communications.

**Table 1. Emergency communications List of Standards[113]**

| No | Group | Document title | Scope of document | Status |
|---|---|---|---|---|
| **1** | ITU | **Compendium on Emergency Telecommunication** | Compendium of ITU'S Work on Emergency Telecommunications | Published (2007) |
| **2** | ITU-D | Question 25/2 Access technology for broadband telecommunications including IMT, for developing countries | This Report covers technical issues involved in deploying broadband access technologies by identifying the factors influencing the effective deployment of such technologies, as well as their applications, with a focus on technologies and standards that are recognized or under study within ITU-R and ITU-T. | Published (2014) |
| **3** | ITU-R | Recommendation M.1042 Disaster communications in the amateur and amateur-satellite services | It provides guidance on the roles of the amateur and amateur satellite services in providing communications during disaster situations. | Published (3/2007) |
| **4** | ITU-R | Recommendation M.1637 Global cross-border circulation of radiocommunication equipment in emergency and disaster relief situations | It offers guidance to facilitate the global circulation of radiocommunication equipment in emergency and disaster relief situations including the need for plans and procedures to be in place before a possible disaster event in order to facilitate the speedy authorization of the use of such equipment. | Published (6/2003) |
| **5** | ITU-R | Recommendation M.2015 Frequency arrangements for public protection and disaster relief radiocommunication systems in UHF bands in accordance with Resolution 646 (Rev.WRC-12) | It provides guidance on frequency arrangements for public protection and disaster relief radiocommunications in certain regions in some of the bands below 1 GHz identified in Resolution 646 (Rev.WRC-12). | Published (2/2015) |
| **6** | ITU-R | Recommendation M.2009 | It identifies radio interface standards applicable for public protection and disaster relief (PPDR) operations in some parts of the UHF band. | Published (2/2015) |

113 At the time of this writing, eight deliverables have been produced by the FG-DR&NRR, as shown in Table 1. ITU-T SG2 is considering five such deliverable, namely: [FG-Overview], [FG-Frame], [FG-Gap], [FG-Term] and [FG-DR]; and ITU-G 15 two deliverables, [FG-NRR] and [FG-MDRU].

| | | | | |
|---|---|---|---|---|
| | | Radio interface standards for use by public protection and disaster relief operations in some parts of the UHF band in accordance with Resolution 646 (WRC-03) | | |
| **7** | ITU-R | Recommendation M.1826 Harmonized frequency channel plan for broadband public protection and disaster relief operations at 4 940-4 990 MHz in Regions 2 and 3 | It addresses harmonized frequency channel plans in the band 4 940-4 990 MHz for broadband public protection and disaster relief radiocommunications in Regions 2 and 3. | Published (10/2007) |
| **8** | ITU-R | Recommendation M.1746 Harmonized frequency channel plans for the protection of property using data communication | It addresses system interoperability and harmonized frequency channel plans for the protection of property using data communication. | Published (3/2006) |
| **9** | ITU-R | Report ITU-R M.2085 Role of the amateur and amateur-satellite services in support of disaster mitigation and relief | It is intended to document the role of the amateur and amateur-satellite services in provision of radiocommunications in support of disaster mitigation and relief. It includes information developed after the South-East Asia tsunami in December 2004. | Published (11/2011) |
| **10** | ITU-R | Report M.2117 Software-defined radio in the land mobile, amateur and amateur-satellite services | It addresses the application and implications of software defined radio to mobile systems, including, but not limited to, IMT-2000 and systems beyond, dispatch systems, intelligent transport systems (ITS), public mobile systems including public protection and disaster relief (PPDR), and first and second generation cellular systems including their enhancements. It addresses issues on the efficient use of spectrum using SDR techniques and adaptive control mechanisms, frequency sharing issues relating to SDR and general technical issues. | Published (11/2012) |
| **11** | ITU-R | Report ITU-R M.2033 Radiocommunication objectives and | It defines the PPDR objectives and requirements for the implementation of future advanced solutions to satisfy the operational needs of PPDR organizations around the year 2010. Specifically, it identifies objectives, | Published (9/2003) |

| | | | | |
|---|---|---|---|---|
| | | requirements for Public Protection and Disaster Relief (PPDR) | applications, requirements, a methodology for spectrum calculations, spectrum requirements and solutions for interoperability. | |
| **12** | ITU-T | **E.107**<br>Emergency Telecommunications Service (ETS) and interconnection framework for national implementations of ETS | This Recommendation provides guidance that will enable telecommunications between one ETS national implementation (ENI) and other ENI(s) (authority-to-authority), in addition to providing a description of ETS.<br>Early warning (EW) for disasters is not part of this Recommendation, but is left for future studies that may add to this Recommendation or become a separate Recommendation. | Published (02/2007) |
| **13** | ITU-T | **E.108**<br>Requirement for disaster relief mobile message service | The intent of a disaster messaging service is to allow an alternate method to communicate safety status information. Two approaches are presented. The first is a text-based messaging system, and the second is a voice-based messaging system | To be Published (http://www.itu.int/ITU-T/recommendations/rec.aspx?rec=E.108 ) |
| **14** | ITU-T | **E.161.1**<br>Guidelines to select Emergency Number for public telecommunications networks | This Recommendation is intended for use by Member States who are in the process of selecting:<br>• a) a single emergency number for the first time<br>• b) a secondary alternative emergency number.<br>Either emergency number will be made available to users and subscribers, and therefore the mapping of these numbers to technology requirements is considered out of scope of this Recommendation.<br>In the long run, this Recommendation will contribute to globally harmonized emergency numbers. | Published (09/2008) |
| **15** | ITU-T | **M.3350**<br>TMN service management requirements for information interchange across the TMN X interface to support provisioning of Emergency Telecommunication Service (ETS) | The subject of this Recommendation is the interface between a duly authorized service customer (SC) and a duly authorized service provider (SP) that is used to manage emergency telecommunication service (ETS) features. ETS features are used by emergency responders during disaster events for telecommunications to organize and coordinate activities for saving lives and restoring community infrastructure. The definition of actual ETS features and requirements are the subject of other Recommendations.<br>This Recommendation describes the ETS Management Service (ETSMS) and identifies functional requirements for interchange of critical service management information, which relates to ETS features, among TMNs across the X-interface of the service management layer as defined by ITU-T Rec. M.3010. The requirements described will enable authorized disaster | Published (05/2004) |

| | | | | |
|---|---|---|---|---|
| | | | response and recovery operations personnel, as SCs, to interact with SPs to share knowledge of the availability of services, configure services, and activate required services. Some aspects of the ETSMS may be used at any time independent of the occurrence of actual emergencies.<br>Other TMN Recommendations will cover the specific format and data elements as well as the protocols for interchange of management information across the X-interface for the ETSMS. | |
| **16** | ITU-T | **Y.1271**<br>Framework(s) on network requirements and capabilities to support emergency telecommunications over evolving circuit switched and packet-switched networks | Contextual understanding and careful thought is required to address the unique challenges faced by emergency telecommunications. This Recommendation presents an overview of the basic requirements, features, and concepts for emergency telecommunications that evolving telecommunication networks are capable of providing. This Recommendation provides guidance to telecommunication network operators on network requirements and capabilities to support emergency telecommunications offerings and should provide responders (users) with useful information for (acquisitions) request of such capabilities.<br>NOTE – This Recommendation defines requirements for networks which when implemented should help support emergency telecommunication services and facilitate the application of ITU-T Rec. E.106 if needed. | Published (10/2004) |
| **17** | ITU-T | **Y.2205**<br>Next Generation Networks – Emergency telecommunications – Technical considerations | This Recommendation specifies technical considerations that can optionally be applied within the next generation network (NGN) to enable emergency telecommunications (ET). In addition, this Recommendation also outlines the underlying technical principles involved in supporting ET. It specifies requirements and capabilities for ET beyond the ones specified in [ITU-T Y.2201] in the context of NGN (as defined in [ITU-T Y.2001] and further outlined in [ITU-T Y.2011]).<br>Emergency telecommunications (including support of some aspects of early warning (see Figure 1)) include:<br>• individual-to-authority emergency telecommunications, e.g., calls to emergency service providers;<br>• authority-to-authority emergency telecommunications;<br>• authority-to-individual emergency telecommunications, e.g., community notification services.<br>Appendix I provides additional information for the above listed ET categories. | Published (05/2011) |

| | | | | |
|---|---|---|---|---|
| | | | Some requirements and capabilities for early warning are also specified. Individual-to-authority emergency telecommunications capabilities are not addressed and are outside the scope of this Recommendation.<br>Some of the technical means described herein could also be used for individual-to-authority or individual-to-individual emergency telecommunications; however, these categories are not addressed in this Recommendation. | |
| **18** | ITU-T | **Y.2705**<br>Minimum security requirements for the interconnection of the Emergency Telecommunications Service (ETS) | This Recommendation provides the minimum security requirements for the inter-network interconnection of ETS. The scope of the security requirements includes the integrity, confidentiality and availability protection for ETS communications across network boundaries (i.e., between different national networks).<br>The purpose of this Recommendation is to provide a minimum set of security requirements that can be used to facilitate the support of ETS across directly or indirectly interconnected networks. | Published (03/2013) |
| **19** | ITU-T | **X.1303 bis**<br>Common alerting protocol (CAP 1.2) | The common alerting protocol (CAP) is a simple but general format for exchanging all-hazard emergency alerts and public warnings over all kinds of networks. CAP allows a consistent warning message to be disseminated simultaneously over many different warning systems, thus increasing warning effectiveness while simplifying the warning task. CAP also facilitates the detection of emerging patterns in local warnings of various kinds, such as an undetected hazard or hostile act might indicate. CAP also provides a template for effective warning messages based on best practices identified in academic research and real-world experience | Published (03/2014) |
| **20** | FG-DR&NRR | **FG-DR&NRR**<br>Deliverable<br>Overview of Disaster Relief Systems, Network Resilience and Recovery | This deliverable provides an overview of Disaster Relief Systems (DR), Network Resilience and Recovery (NRR). Disaster Relief Systems provide the users with telecommunication services to mitigate the damage caused by the disaster before, during, and after the disaster incident. Network Resilience means the robustness of the network infrastructure and the continuity of the telecommunication services despite damage caused by the disaster. Network Recovery restores the network infrastructure and telecommunication services to their original status or to a certain level of availability even temporarily to provide the users with services after a disaster.<br>The objective of this deliverable is to describe the following: | Technical Report (05/2014) |

| | | | | |
|---|---|---|---|---|
| | | | • Overview of expected study areas, categorization, and definition of terminologies<br>• Brief introduction of activities of ITU and other organizations relevant to DR&NRR.<br>• Summary of contents of other major deliverable documents in the Focus Group. | |
| **21** | FG-DR&NRR | **FG-DR&NRR** Deliverable Promising technologies and use cases | Based on the contributions to FG-DR&NRR meetings, this document provides an integrated view of promising technologies for Disaster Relief Systems, Network Resilience and Recovery (DR&NRR). First, an integrated view of DR&NRR technologies is described that allows the support of rescue organizations as well as private persons when disasters occur (Part I). This is followed by descriptions of each technology component explicitly mentioned in the integrated view (Part II). Other technologies, which do not fit into the single pictorial view but that appear promising are also described (Part III).<br>Information about FG-DR&NRR inputs is also briefly summarised (Part IV) and references provided using a common formal template (Part V). | Technical Report (05/2014) |
| **22** | FG-DR&NRR | **FG-DR&NRR** Deliverable Gap Analysis of Disaster Relief Systems, Network Resilience and Recovery | As stipulated by the Terms of Reference of the Focus Group this document constitutes a deliverable on performing a gap analysis of the standardization work on disaster relief systems, network resilience and recovery. The document aims at providing a living list of standards bodies, forums, and consortia dealing with aspects of telecommunication/ICT, including information concerning their activities and documents related to disaster relief systems, network resilience and recovery and also at identifying:<br>• Existing standardization work catering to the requirements<br>• The requirements that have not been met by the present state of standardization and finding a way to meet them.<br>Based on above, this document identifies and proposes work that needs to be carried out within ITU. | Technical Report (05/2014) |
| **23** | FG-DR&NRR | **FG-DR&NRR** Deliverable Terms and definitions for disaster relief systems, network resilience and recovery | This document contains terms and definitions relevant to providing a common general understanding in the area of disaster relief systems, network resilience and recovery. It also intends to support the harmonized creation of terms and definitions in this area. | Technical Report (05/2014) |

| | | | | |
|---|---|---|---|---|
| **24** | FG-DR&NRR | **FG-DR&NRR** Deliverable Requirements for Disaster Relief System | This deliverable describes requirements for a Disaster Relief System including an Early Warning System, which are used for real and potential victims (note), before, at or during and after disasters.<br>NOTE – The word "victim" in this document is the person who affected by the disaster. | Technical Report (05/2014) |
| **25** | FG-DR&NRR | **FG-DR&NRR** Deliverable Requirements for network resilience and recovery | This deliverable describes requirements for network resilience and recovery before, at or during and after disasters. | Technical Report (05/2014) |
| **26** | FG-DR&NRR | **FG-DR&NRR** Deliverable Requirements on the improvement of network resilience and recovery with movable and deployable ICT resource units | This Document shows key factors for examining various usage scenarios of movable and deployable ICT resource units (MDRUs) and introduces one promising use of the MDRU as a local node. Focusing on this use, this Document describes design principles for the MDRU and its requirements, which will impact subsequent standardization works.<br>One of the purposes of this Document is to identify MDRU-related issues for facilitating a future, full-fledged, standardization work and by gathering them into a single Document. | Technical Report (05/2014) |

## 4.3 Environmental issues

### 4.3.1. Overview[114]

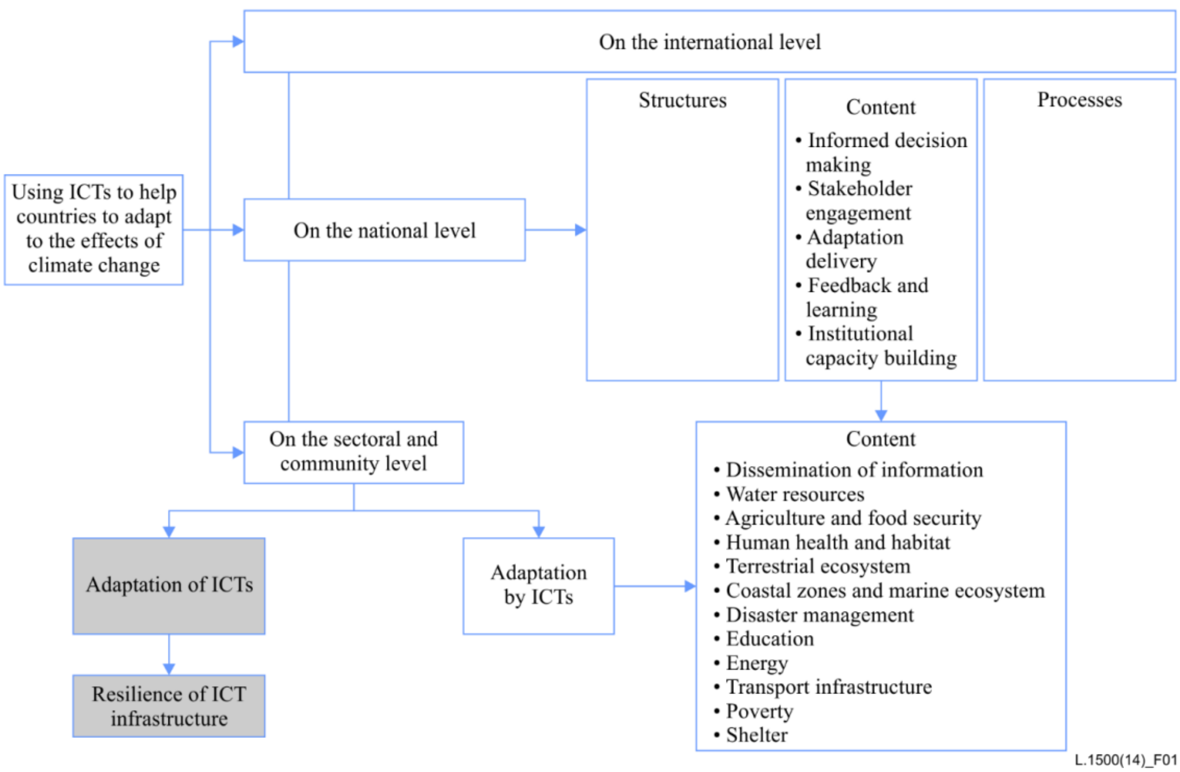
- **Climate change**

ICTs deliver innovative products and services which are transforming the way human societies live. At the same time, ICTs enable other sectors, such as administration, instructions, commerce, manufacturing, logistics, buildings, electric grids and other utilities (e.g. water), to develop and work in a more efficient mode.

On the other hand, the adverse effects of climate change pose a threat to the development and sustainability of the ICT sector and related sectors. To ensure environmental sustainability of the ICT sector and other sectors, it is important to develop adaptation strategies to address the effects of climate change. There are key areas of action to be considered in the design of ICTs and climate change adaptation and mitigation strategies, including policy development and the establishment of adequate structures and processes. At the sectoral level, sector-specific strategies need to be developed to ensure environmental sustainable development in the face of climate variability and change.

ICTs therefore have a strategic role to play in ensuring the adaptability of other sectors. Furthermore, the ICTs themselves are vulnerable to the effects of climate change and should strategically evolve to adapt infrastructure to such changes. This can be done at several levels, from the international, national, sectoral and community level, as shown in Figure 4-3-1.

**ICT and climate change adaptation framework**




[114] ITU-T L.1500 (Framework for information and communication technologies (ICTs) and adaptation to the effects of climate change), ITU-T Focus Group on Smart Sustainable Cities Deliverables

Figure 4-3-1. ICTs and a framework for adaptation to climate change[115]

The differences in strategic approach at various levels, and between the ICT sector and other sectors, bring out a need for several adaptation approaches specific to the ICT sector and for countries to use.

- **Smart Sustainable Cities**

Cities are powerful engines of economic growth, fuelled by intensive interpersonal communication and high concentrations of specialized skills. Urbanization's advantages are however mirrored by significant sustainability challenges, with cities today accounting for over 70 per cent of global greenhouse gas (GHG)[116] emissions and 60-80 per cent of global energy consumption. Cities also produce 50% of the global waste. As approximately 80 percent of the global GDP is generated in cities, urbanization has the potential to contribute to sustainable growth if managed properly by allowing innovation and new ideas to emerge. Additionally, as an estimated 70 per cent of the world's population will live in cities by 2050, sustainable urbanization has also become a key policy point for administrations across the world.

With the growing urban needs, there is increasing pressure on resources including water, land and fossil fuels. There are also growing concerns regarding transportation infrastructure, providing adequate healthcare, establishing credible waste management systems, access to education and safety for the growing population of urban residents.[117]

Here, ICTs have a crucial role to play by increasing environmental efficiency across industry sectors and enabling such innovations as intelligent transport systems (ITS) and "smart" water, energy and waste management.

In light of the above, the concept of Smart Sustainable Cities (SSC) developed by ITU and UNECE has gained significant recognition. SSC leverage the potential of ICTs in urban administration systems to create cities which are not only economically, culturally, socially advanced but are also designed to achieve environmental sustainability.

An internationally accepted definition for Smart Sustainable Cities was agreed to under the umbrella of ITU-T Study Group 5 on Environment and Climate Change:

*"A smart sustainable city is an innovative city that uses information and communication technologies (ICTs) and other means to improve quality of life, efficiency of urban operation and services, and competitiveness, while ensuring that it meets the needs of present and future generations with respect to economic, social, environmental as well as cultural aspects".* (ITU-UNECE, 2015)

ITU together with UNECE has also developed an extensive list of key performance indicators (KPIs) to assist urban stakeholders in smart city transitions.

In addition to traditional ICT infrastructures such as Network Infrastructure, Software Applications, Cloud Computing / Data Platforms and Access Devices., the following table is a sample list (not exhaustive) of communications related technologies which have relevance to Smart Sustainable cities.

Table 4-3-1: A sample list of ICT related to Smart Sustainable Cities

| Infrastructure Topic | Technologies |
|---|---|
| Building Management | • Building Automation |

[115] The diagram is based on ITU-T Report (2012), *Information and communication technologies (ICTs) and climate change adaptation and mitigation: The case of Ghana 2012*. http://www.itu.int/dms_pub/itu-t/oth/4B/01/T4B010000020001PDFE.pdf

[116] The ITU-T Y.2200-series - Greenhouse gas monitoring services provided over NGN, 2013 - describes general aspects of the GHG monitoring issue, and it provides requirements and required functions. In addition, a service model and functional architecture for a GHG monitoring service are presented. NGN-based GHG monitoring service scenarios are also presented

[117] ITU-T Focus Group on Smart Sustainable Cities.- Technical Report on "Smart sustainable cities: a guide for city leaders"

| Infrastructure Topic | Technologies |
|---|---|
| | • Building Control<br>• IT Network Systems<br>• Building facilities (energy, heat, air, water...)<br>• Crisis Management Solution (power, infrastructure damage...) |
| Data Communications & Security | • Voice/Video/Data<br>• Audio Visual<br>• Structured Cabling<br>• TCP/IP/BAS Protocols<br>• Remote VPN Access<br>• Computer Access<br>• Network Access<br>• Firewalls<br>• Managed Security Services<br>• Mobile Broadband<br>• Mobile Security<br>• Data Security Infrastructure |
| Smart Grid / Energy / Utilities | • Energy Logistics<br>• Distribution (electricity, water, gas, heat)<br>• Utility Monitor<br>• Lighting<br>• Back-Up Power<br>• Leakage Monitor<br>• Waste treatment including water |
| Physical Safety and Security | • Access Control<br>• Video Surveillance Intrusion Detection<br>• Biometrics<br>• Perimeter and Occupancy Sensors<br>• Fire Alarm Panels<br>• Detection (Smoke/Heat/Gas/Flame)<br>• Fire suppression<br>• Notification and Evacuation |
| Emergency Response | • Integrated Fire Department<br>• Police and Medical Services<br>• Centralised and Remote Command and Control<br>• Scalable Decision Making Process |
| Traffic and Transportation (Mobility) | • Traffic Control & Monitoring (rail, underground, buses, personal vehicles)<br>• 24/7 Supply Management (logistics) |

### 4.3.2. Role and Key Areas of ICT infrastructure for Smart Sustainable Cities[118]

- **Climate change impact in cities**

[118] ITU-T Focus Group on Smart Sustainable Cities Deliverables: Technical Report on Information and communication technologies for climate change adaptation in cities.

Climate change refers to a change of climate that is attributed directly or indirectly to human activity that alters the composition of the global atmosphere and that is in addition to natural climate variability observed over comparable time periods. These changes will lead to wide ranging impacts across cities.

Climate change has a range of short-term and long-term consequences on cities. It will have both direct and indirect impacts on human health, physical assets, economic activities, and social systems depending on how well prepared a city is and how it responds.

Climate change is likely to affect human health in cities, either directly or indirectly (Table 4-3-2) from physiological effects of heat and cold or indirectly, through for instance the transmission of vector-borne pathogens or effects on well-being from flooding.

- **The role of ICTs in cities' climate change adaptation**

ICT tools and services can support the policy process covering all phases of the emergency and adaptation planning (risk mapping, risk reduction, capacity building and community involvement). These adaptation strategies require robust ICT infrastructures and also specific standards to enhance its use. Different types of disasters and adaptation challenges may require different ICTs solutions and standardization requirements. Not only communication technologies and infrastructure are required for effective inclusion of ICTs in city adaptation programs. Also the development of ICT standards plays an essential role in helping strengthening cities' response to climate change adaptation worldwide.

Considering this, ICTs use for climate change adaptation and disaster management can be grouped in three categories of strategies as follows. [119]

- **ICTs for climate enhanced disaster risk management (DRM)**

  Climate Change Action Plans in cities include adaptation strategies based on Disaster Risk Management (DRM) programs.

  These provide a well-proven framework and tool-set for cities in order to address natural disasters and helps cities explore strategies before disaster occurs, during disasters, and after disasters. ICTs facilitate communication and exchange of information between local governments, communities and all relevant stakeholders involved in the climate DRM processes.

  Table 4-3-3 describes some examples of ICT based services to support DRM processes in cities.

- **ICTs for city resilience & adaptive capacity**

  City Resilience can be achieved in two ways: by making urban systems more robust and by increasing adaptive capacity.

- **ICT-based adaptation informed decision making**

  ICTs can help to strengthen institutional and capacity development (e.g., through online training, improved knowledge access) to inform the implementation of sectoral and local programmes.

[119] ITU-T Focus Group on Smart Sustainable Cities- Technical Report on Information and communication technologies for climate change adaptation in cities

Table 4-3-2. Examples of Climate change direct and indirect impacts in cities[120].

| Projected climate change impacts | Likelihoods | Direct impacts | Indirect impacts | Geographical location affected |
|---|---|---|---|---|
| **Warmer with fewer cold days and nights, more hot days and nights** | Virtually certain | Exacerbation of urban heat island effect increase risk of related mortality | Declining Air quality | Inland cities and cities reliant on snowpack for water supply |
| **Hot spells/heat weaves increased frequency** | Very likely | Increase demand for cooling and reduced energy demand for heating Greater stress on water resources included those that rely on snowmelt from increased water demand and declining water quality | Energy transmission and distribution maybe overstressed Wider geographical incidence of vector bone diseases ( for example malaria) Less disruption to transport from snow and ice | Inland cities and cities reliant on snowpack for water supply |
| **Heavy precipitation events increased frequency** | Very likely | Flooding, strong winds and landslides Disruption of public water supply | Withdrawal of risk coverage in vulnerable areas by private insures | Coastal and port cities, those on riverbanks or marginal land in floodplains, mountains regions |
| **Intensity of tropical cyclone activity increases** | Likely | Damage and losses of physical assets and infrastructure Increased risk of death , injuries and illnesses Disruption of transport, commerce and economic activities | | Coastal and port cities. |
| **Areas affected by drought increase** | Likely | Stress on water resources Reduced energy supply from hydropower Land degradation with lower agricultural yields, increased risk of food shortage and dust storms | Water quantity and quality for consumption and food production Population migration | Cities in unused to arid conditions |
| **Rising sea level** | Virtually certain | Permanent erosion and submersion of land Cost of coastal protection or coast of relocation Decreased ground water availability Increase salinity in estuaries & coastal aquifers Effects of tropical cyclones and storm surges, particularly coastal flooding | Recreational activities affection | Coastal cities |

[120] Source: compiled from World Bank (2011) and Hunt and Watkiss (2011)

Table 4-3-3. Examples of ICT use for DRM in cities[121]

| Disaster phases | ICT Services involved | Major tasks |
|---|---|---|
| DISASTER PREVENTION *Prediction and detection* | • Meteorological services (meteorological aids and meteorological-satellite service)<br>• Earth exploration-satellite service<br>• Geographic Information Systems (GIS)<br>• Blogging, web 2.0 and social networking | • Weather and climate prediction<br>• Detection and tracking of hurricanes, typhoons, forest fires, etc.<br>• Providing warning information |
| EMERGENCY PREPARDNESS & RESPONSE *Alerting* | • Amateur services<br>• Broadcasting services terrestrial and satellite (radio, television, etc.)<br>• Fixed services terrestrial and satellite<br>• Mobile services (land, satellite, maritime services, etc.)<br>• Blogging, web 2.0 and social networking | • Receiving and distributing alert messages<br>• Disseminating alert messages and advice to large sections of the public<br>• Delivering alert messages and instructions to telecommunication centers for further dissemination to public<br>• Distributing alert messages and advice to individuals |
| RECOVERY *Relief* | • Amateur services<br>• Broadcasting services terrestrial and satellite (radio, television, etc.)<br>• Earth exploration-satellite services<br>• Fixed services terrestrial and satellite<br>• Mobile services (land, satellite, maritime services, etc.)<br>• Blogging, web 2.0 and social networking | • Assisting in organizing relief operations in areas (especially when other services are still not operational)<br>• Coordination of relief activities by disseminating information from relief planning teams to population<br>• Assessment of damage and providing information for planning relief activities<br>• Exchange of information between different teams/groups for planning and coordination relief activities<br>• Exchange of information between individuals and/or groups of people involved in relief activities |

Adaptive capacity is the ability to respond to change and surprise, to quickly learn and easily adapt to new conditions without any major costs or permanent loss in function.

Within this approach, cities will become forward-looking and adaptation programs can emphasize preventive rather than reactive measures.

- ICTs for adaptation capacity building and community involvement

In addition to monitoring the environment and the changing climate, ICTs have a role to play in cities' climate change adaptation by facilitating information dissemination.

Tools such as online training, blogging or web 2.0 tools; can contribute to disseminate knowledge and strengthen capacity of the experts involved in the process of resilience building and disaster risk management programs.

[121] Source: Adapted from ITU-R (2013) and LinnerAsia (2008)

### 4.3.3. Smart Sustainable Cities (SSC) Infrastructure[122]

- **Digital/ICT Infrastructure For SSC**

Technical aspects related to the different layers of ICT Infrastructure that can be identified will be included in this section of the document, such as those that appear in the following image below:

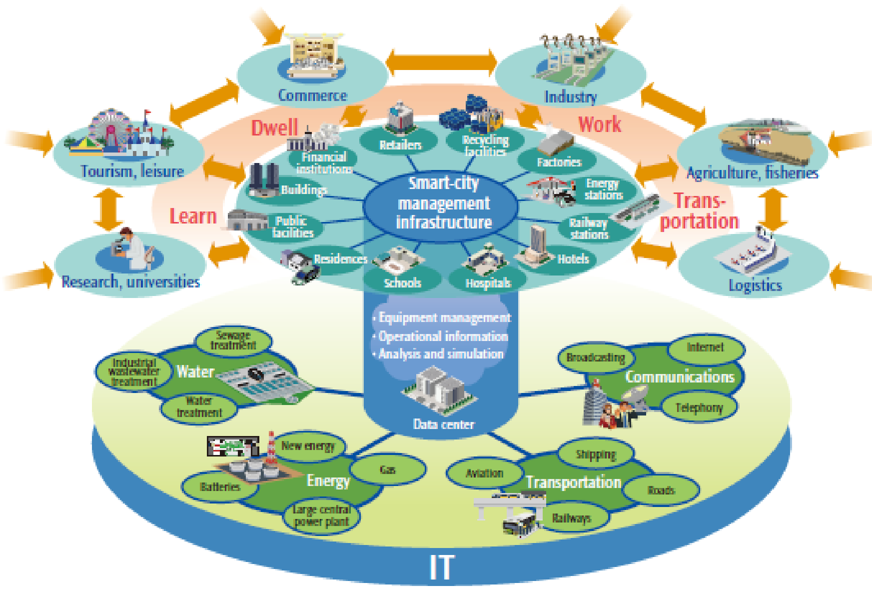



Figure 4-3-2. Smart city management infrastructure (Source: Hitachi)

From the point of view of the ICT infrastructure two aspects shall be considered: Network Facilities and his layers, and ICT Facilities.

In the most classic sense of the concept of network services, describes both the data layer and the layer of communications.

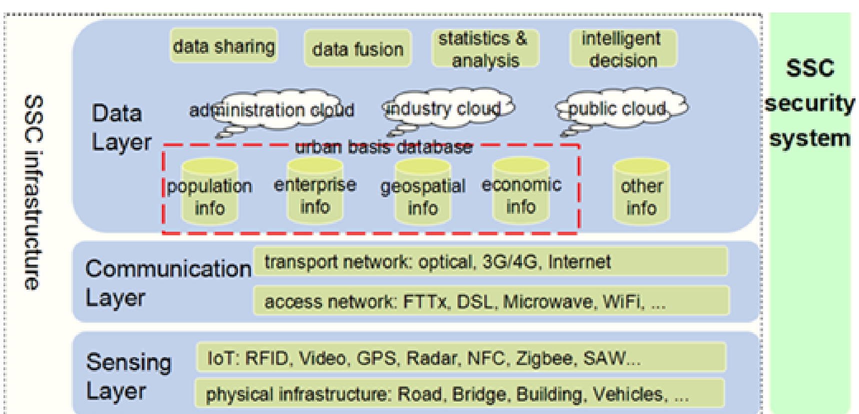



Figure 4-3-3. SSC Infrastructure

122 ITU-T Focus Group on Smart Sustainable Cities Deliverables. http://itu.int/go/HIRR .

- **Data Layer**

Those centralized repositories, for the storage, management, and dissemination of data and information organized around the objective Sustainable Smart City (SSC). It is recommended that data warehouses use a platform that is scalable, reliable and high performance that allows you to grow as you increase the number of sensors installed in the territory and the city.

The infrastructure must be designed and provisioned considering the specific volumetric for supporting the business applications and considering the peak load transaction in jobs per second, availability and scalability requirements. When volumetric and projected growth do not manifest as envisaged, this method of sizing infrastructure compute and storage could lead to either undersizing or oversizing the footprint. Often, having such islands of computer infrastructure and storage, leads to underutilization of resources. This has a cascading effect on investment and effort spent toward energy consumption, management overheads, software licenses and data center costs.

A data center is a facility used to house computer systems and associated components, such as telecommunications and storage systems. It generally includes redundant or backup power supplies, redundant data communications connections, environmental controls (e.g., air conditioning, fire suppression) and various security devices.

- To be able to reduce the overall power consumption:

  Power Usage Effectiveness (PUE) is often used as an indicator to measure the energy effectiveness of air-conditioning of data centres. PUE is ratio between power consumption of overall data centre and that of ICT equipment in the data centre. If the figure of PUE gets lower, it means the effectiveness gets increased. Because electricity consumption for internal fans is counted as that of ICT equipment, the larger the internal fans are, the smaller PUE is and the better the energy effectiveness appears. In contrast to this, it is required to reduce the overall power consumption of data centres, not to limit to lower PUE values.

- To be able to use regardless of climate conditions:

  Temperature or humidity of external ambient air varies according to locations and seasons. It is required to be able to reduce power consumption in a wide range of temperatures and humidity levels on the earth.

Data center infrastructure management (DCIM) is the integration of information technology (IT) and facility management disciplines to centralize monitoring, management and intelligent capacity planning of a data center's critical systems. Achieved through the implementation of specialized software, hardware and sensors; DCIM enables common, real-time monitoring and management platform for all interdependent systems across IT and facility infrastructures.

Depending on the type of implementation, DCIM products can help data center managers identify and eliminate sources of risk to increase availability of critical IT systems. DCIM products also can be used to identify interdependencies between facility and IT infrastructures to alert the facility manager to gaps in system redundancy, and provide dynamic, holistic benchmarks on power consumption and efficiency to measure the effectiveness of "green IT" initiatives.

Measuring and understanding important data center efficiency metrics. A lot of the discussion in this area has focused on energy issues, but other metrics can give a more detailed picture of the data center operations. Server, storage, and staff utilization metrics can contribute to a more complete view of an enterprise data center. In many cases, disc capacity goes unused and in many instances the organizations run their servers at 20% utilization or less. More effective automation tools can also improve the number of servers or virtual machines that a single admin can handle.

- **Communication Layer**

It is one of the main aspects of the ICT infrastructure, it should be noted both the national infrastructure and the specifically urban, since the backhauls will feed the backbones that are bound to the international links. Access networks are keys for the development of SSC; however they are having problems in many cities, especially in matters related to the deployment of antennas.

The convergence of infrastructure already introduced earlier should be considered carefully for this type of transport of data networks in urban environments.

To transport the large amount of data that handled the smart cities will be necessary for local governments implement national policies to deploy broadband networks.

In some cases, it is difficult to lay cables. Such cases include providing services around waterway crossings and between buildings. In other cases, it is not efficient to lay cables. Such cases include providing services for use at temporary events and for rapid network recovery in emergency occasions like big natural disasters.

- To consume less electricity

  It is required to consume less electricity per unit amount of transmission of data in order to reduce the environmental burden

  It is also required to use less electricity when some data is transmitted along the same distance

  It is preferable to be able to obtain electricity autonomously using natural energy such as wind power and energy from sunlight

- To be small and lightweight

  It is required to be easily installed and used for temporary radio relays or live broadcast from the events sites as well as the means of rapid network recovery in emergency where mobility characteristic is required

  It is preferable to be able to lessen the number of component parts or the amount of volume to contain in order to reduce the environmental burden. For example, impulse radio wireless technology allows the system not to use oscillators which are likely to be large-size.

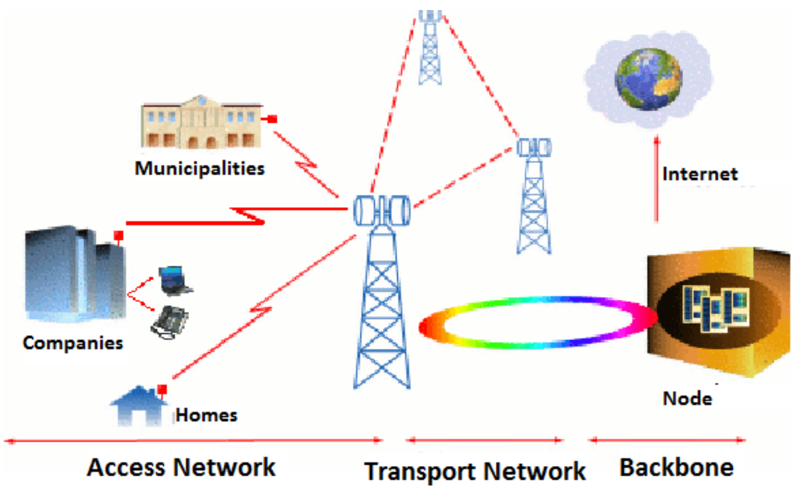



Figure 4-3-4. Communication layer

- **Sensing Layer**

  This layer consists of terminal node and capillary network. The terminals (sensor, transducer, actuator, camera, RFID tag, barcode symbols etc.) sense the natural environment where the smart sustainable city is located and the corresponding hard infrastructure and utilities (water, transport etc.). It provides the superior 'environment-detecting' ability and intelligence for monitoring and controlling the physical infrastructure within the city. The capillary network connects various terminals to communication layer, or directly to data layer and/or application layer providing ubiquitous and omnipotent information and data.

- **Technologies Used in Integrated Management for Smart Sustainable Cities**

In general, the objects of the integrated management for smart sustainable cities are the people, events, things, and the corresponding information streams. People can analyze, use and manage all kinds of information streams, that is to say, people can manage all kinds of things intelligently, and realize the smart decision making and judgments on them. As the people, events and things are from multiple systems, they need to be managed comprehensively.

Compared with the digital city management, from the technical level, the integrated management for smart sustainable cities is to realize the transformation from the online management based on the internet to the real-time dynamic management on the basis of Internet of Things (IoT) [123], from the sensing management of every single sensor to the collaborative management of multiple sensors, from the island of the industrial model management to the model web management of the application decisions.

To be specifically, the integrated management for smart sustainable cities consist of the observation web, service web, and model web technologies.

The observation web technology aims at breaking through the barriers of the multiple and heterogeneous observing and sensing modes, and implements the automatic, real-time, and comprehensive sensing about the city management and operating status via the web, sensing, and intellectual technologies.

The service web technology is to overcome the obstacles in the workflow and geospatial sensor web technologies, and to achieve the goal of network intelligent service which is in accordance with specific sensor actions and interface specifications.

The model web technology is to hurdle the bars in the meta-modeling as well as catalog registration technology, and to bridge the communication gaps between the heterogeneous sensors, models, as well as simulation and decision support systems. The model web technology could be used to solve the problems in the expression, understanding, sharing and cooperation of the heterogeneous city decision models. Clients could realize the city integrated emergency decision by combining and optimizing these models on decision terminals.

#### 4.3.4. Green Data Centres[124]

In order to improve the energy efficiency of data centres, it is necessary to consider all stages from design through to construction. Even after the building of data centres is complete, they must continue to be managed and maintained to ensure efficient energy consumption.

- Planning, utilization, and management

  It is important to develop a holistic strategy and management approach to the data centre to support economic efficiency and environmental benefits.

  – Involvement of organizational groups: Effective communication between different departments working in the data centres is crucial to ensure efficiency and thereby avoid capacity and reliability issues. To ensure effective communication, the following steps are proposed:
  – General policies: These policies apply to all aspects of the data centre and its operation.
  – Resilience level and provisioning: One of the most significant sources of inefficiency in a data centre is the over-provision of space, power or cooling, and the use of existing facilities at partial capacity. Monolithic design, as opposed to modular design, of facilities is also frequently an unnecessary capital expenditure.
- ICT equipment and services

  ICT equipment creates the demand for power and cooling in the data centre. Any reduction in power and cooling used by, or provisioned for ICT equipment will have magnified effects for the utility energy supply.

  The purpose of environmental specifications of equipment is to ensure that new equipment is capable of operating under the wider ranges of temperature and humidity, thus allowing the operator a greater flexibility in operating temperature and humidity.

  – Selection of new ICT equipment
  – Selection of new telecom equipment
  – Deployment of new ICT services
  – Management of existing ICT equipment and services
  – Data management
- Cooling

---

[123] ITU-T Study Group 20 on Internet of Things and its applications including smart cities and communities, is responsible for international standards to enable the coordinated development of IoT, including machine-to-machine communications and ubiquitous sensor networks. The group develops standards that leverage IoT technologies to address urban-development challenges.

[124] ITU-T L.1300 (Best practices for green data centres)

Cooling of the data centre is frequently the largest energy loss in the facility and as such represents a significant opportunity to improve efficiency.

- Airflow design and management
- Cooling management
- Temperature and humidity settings
- Computer room air conditioners
- Re-use of data centre waste heat

• Data centre power equipment

The other major part of the facility infrastructure is the power conditioning and delivery system. This normally includes uninterruptible power supplies, power distribution units, and cabling, but may also include backup generators and other equipment.

Power delivery equipment has a substantial impact upon the efficiency of the data centre and tends to remain operational for many years once installed. Careful selection of power equipment at the design stage, can deliver substantial savings throughout the lifetime of the facility.

• Other data centre equipment

Energy is also used in the non-data floor areas of the facility, in office and storage spaces. Energy efficiency in non-data centre areas should be optimized based on relevant building standards, such as relevant EU standards, LEED, BREEAM, etc.

• Data centre building

The location and physical layout of the data centre building is important to achieving flexibility and efficiency. Technologies, such as fresh air cooling, require significant physical plant space and air duct space that may not be available in an existing building.

- Building physical layout
- Building geographic location

• Monitoring

The development and implementation of an energy monitoring and reporting management strategy is core to operating an efficient data centre.

- Energy use and environmental measurement
- Energy use and environmental reporting
- ICT reporting

• Design of network

It is important to specify requirements on network design to connect equipment present in the data centre and the data centre with other data centres.

• Cloud data centre

The cloud data centre basically requires a more advanced energy-saving approach than the existing data centre due to high density and high integration, from the perspectives of construction, electric power, air conditioning, and other infrastructures. The excessive initial investment cost can be reduced by designing the infrastructure facilities such that phased extension is supported. Moreover, the infrastructure facilities can be operated in an energy-efficient manner by implementing the different availability requirements and power density by module.

Therefore, the dedicated cloud data centre should 1) support a high-density environment, 2) house highly energy-efficient equipment to address the problem of high power consumption and high heat emission, and 3) have the structure of flexibility and scalability to cope with the rapidly changing environment. Lastly, it should have a management system that can control the large-scale ICT resources efficiently and in a cost-effective manner.

• Optimization of energy management of whole data centre

In order to reduce energy consumption of the whole data centres, not only energy efficiency for each device such as ICT devices and air-conditioning equipment but also energy optimization for all devices is important.

### 4.3.5. Energy saving for future networks[125]

- **Background and motivation**

Energy saving in the ICT field is an important issue, as has been identified in designing future networks [ITU-T Y.3001][126]. One of the basic objectives of the development of future networks is demonstrating environmental awareness, which may be realized via energy-saving technologies. Historically, energy saving has been studied for increasing benefits to the user or company, such as reduced energy costs and temperature management for stable machine operation.

The importance of these issues is increasing due to the more widespread implementation of network equipment and the greater energy consumption that this requires. It is also becoming increasingly important from a social aspect to support the reduction of GHG emissions. These issues will gain more importance in the future.

The contribution of ICTs to reduce the negative impact on the environment is often categorized into "Green by ICT" and "Green ICT". "Green by ICT" refers to reducing the environmental impact of non-ICT sectors by using ICTs. "Green ICT" refers to reducing the environmental impact of the ICT itself such as the reduction of electric power consumption of personal computers (PCs), servers, and routers. The contribution of future networks to reducing environmental impact can therefore be categorized as shown below.

- Green by future networks

  A challenge to reduce the environmental impact in non-ICT sectors by using future networks.

  Future networks must become a useful tool for reducing the environmental impact of other sectors. Network architecture designed for smart grids for electric power distribution, or ubiquitous sensor networks that monitor environmental changes of the Earth are a few examples of how "Green by Future Networks" may be interpreted.

- Green future networks

  A challenge to reduce the environmental impact of future networks.

  The fundamental principle for future networks is that they must have a minimum impact on the environment. The use of networks may provide the means to reduce the environmental impact of other sectors. Yet by doing so, it increases the volume of traffic flowing into networks, increases energy consumption of the networks accordingly, which then increases the environmental impact. Reducing the energy consumption of network facilities such as routers, switches and servers is a direct example of contributions of "Green Future Networks".

To reduce energy consumption, it is important to analyse energy consumption at each stage of the lifecycle. In life-cycle management, the following stages are typically used for analysis:

- Production (preparing raw materials and components for the target);
- manufacturing;
- use;
- disposal/recycling.

In the case of networks, the first stage, production, is the preparation of raw materials for small electronic devices and the composition of the equipment that is included. The second stage, manufacturing, includes constructing a network by means of the equipment. For network construction, relevant pieces of equipment are transported from a manufacturer's site to the construction location. The third stage, use, refers to operating the equipment. At the end of the service life of the network, the network including all the equipment would be disposed of and/or recycled in the fourth stage, disposal/recycling. Life-cycle management considers all of these stages. In the case of networks, however, the third stage, use, is primarily considered because energy consumption in the "use" stage is usually the major issue for always-on network equipment, and the energy consumption of this stage can be controlled by network architecture, capabilities and operations.

[125] ITU-T Y.3021 Framework of energy saving for future networks, 2012

[126] ITU-T Y.3001 Future networks: Objectives and design goals, 2011

Energy saving within networks includes a variety of technologies. It is unrealistic to rely on a single technology. At the use stage, three levels can be considered along with their relevant technologies, i.e., device-level, equipment-level and network-level.

- Device-level: Technologies which are applied to electronic devices, such as large scale integration (LSI) and memory.
- Equipment-level: Technologies which are applied to one piece of equipment (a set of devices) such as a router or switch[127].
- Network-level: Technologies which are applied to equipment within the whole network (e.g., a routing protocol applied to multiple routers).

Technologies categorized into each level and their combination will change and evolve. Future networks should incorporate these technologies and flexibly adopt their development and evolutions enhance their energy-saving effects.

- **Approaches to energy saving**

- Reduction of required network capacity
  - Reduce the volume of traffic across the whole network
  - Shift the traffic at peak time, which reduces the maximum capacity
- Improvement in network energy efficiency
  - Control device and/or equipment operation according to traffic dynamics
  - Forward traffic with less power

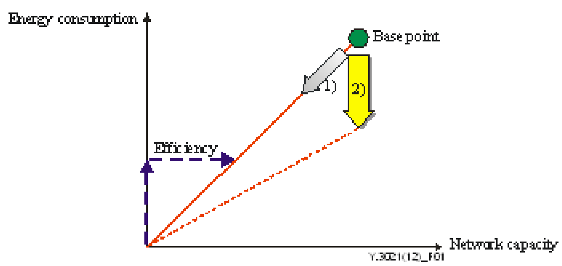



Figure 4-3-7. Energy consumption vs network capacity

- **Possible functions**

[127] For further reference: ITU-T Y.2070 (2015) provides the requirements and architecture of home energy management system (HEMS) and home network (HN) services. ITU-T 2064 (2014) describes requirements and capabilities for saving energy by using smart objects in home networks. It also presents the functional architecture of key components for saving energy through home/building automation.

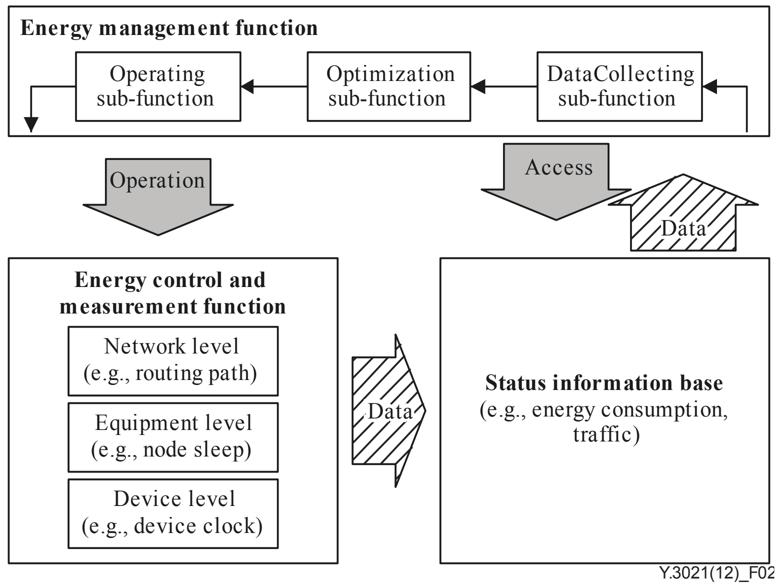



Figure 4-3-8. Possible functions

Figure 4-3-8 shows possible functions for energy saving, including a database and their interactions. These functions can be generally applicable to any energy-saving technology.

- The energy control and measurement function performs control actions to reduce energy consumption, as specified by the energy management function, and obtains measured status information. It is subdivided into device-, equipment-, and network-level technologies.
- The energy management function collects basic information, calculates the optimum case of operation and issues operation commands to the energy control function and the energy measurement function. It includes three subfunctions: DataCollecting subfunction, Optimization subfunction, and Operating subfunction.
- The status information base is a database that gathers basic information of the current mode from the energy control and measurement function. It gives a set of status information such as energy consumption and traffic.

Figure 4-3-8 is a logical figure. The location of the functions and database is basically independent of the specific equipment.

- **High-level requirements**

Energy saving within networks allows network capabilities and their operations to reduce the energy consumption of the network compared with existing networks. It is recommended that the following items are supported:

- Approaches
  – Energy saving within networks is recommended to reduce the volume of traffic to be forwarded by devices or equipment.
  – Energy saving within networks is recommended to shift the traffic at peak time, which reduces the maximum capacity.
  – Energy saving within networks is recommended to control device/equipment operation according to traffic fluctuations.
  – Energy saving within networks is recommended to forward traffic with less power by transmitting data on a simplified mechanism.
- Functions
  – Energy saving within networks is recommended to support the energy control and measurement function, energy management function, and the status information base.
  – The energy control and measurement function is recommended to perform control actions to reduce the energy consumption specified by the energy management function, and to perform the measurement of energy consumption. It is recommended that device, equipment, and network-level technologies are included.

  - The energy management function is recommended to collect basic information, calculate the optimum case of operation, and issue operation commands to the energy control and measurement function. It is recommended that the DataCollecting subfunction, Optimization subfunction, and Operating subfunction are included.
  - The status information base is recommended to gather basic information of the current mode from the energy control and measurement function, such as energy consumption and traffic.
- Influence on network performance
  - When introducing energy-saving technologies, it is recommended that they are applied so that the degradation of network performance (caused by their introduction), falls within the acceptable range for the services.
  - On service provisioning, it is recommended that energy-saving technologies are applied so that the increased consumption, which is caused by multiple simultaneous service provisioning, would fall within the acceptable range in order that individual service requirements are maintained (e.g., delay, loss, etc.).

Environmental issues related ITU-T documents

| No | Group | Document title | Scope of document | Status |
|---|---|---|---|---|
| **1** | ITU-T SG13 | **Y.3021**<br>Framework of energy saving for future networks | This Recommendation:<br>• describes the necessity for energy saving,<br>• reviews potential technologies,<br>• identifies multiple viewpoints to be considered,<br>• identifies major functions and their cyclic interactions,<br>• analyses any possible impact caused by introducing the technologies, and<br>• itemizes high-level requirements;<br>to achieve energy saving within and due to future networks (FNs).<br>The framework and ideas described in this Recommendation may also be applicable and useful for networks which are not categorized as future networks, although the description is produced through full recognition of the objectives and design goals of future networks [ITU-T Y.3001]. | Published (01/2012) |
| **2** | ITU-T SG13 | **Y.3022**<br>Measuring energy in networks | This Recommendation describes a reference model and methods for measuring energy in networks to reduce the operating expenditure (OPEX) of telecommunication network equipment. This Recommendation covers the following:<br>• requirements to measure energy consumption in networks;<br>• reference model and architecture to build an energy measurement framework;<br>• energy efficiency metrics of network elements based on a reference model;<br>• energy consumption measurement methods based on functional architecture. | Published (08/2013) |
| **3** | ITU-T SG5 | **L.1300**<br>Best practices for green data centres | This Recommendation specifies best practices aimed at developing green data centres. A green data centre can be defined as a repository for the storage, management, and dissemination of data in which the mechanical, lighting, electrical and computer systems are designed for maximum energy efficiency and minimum environmental impact. The construction and operation of a green data centre includes advanced technologies and strategies. The Recommendation provides a set of rules to be referred to when undertaking improvement of existing data centres, or when planning, designing or constructing new ones. The proposed best practices cover:<br>• data centre utilization, management and planning;<br>• ICT equipment and services;<br>• cooling;<br>• data centre power equipment;<br>• data centre building; | Published (06/2014) |

| | | | | |
|---|---|---|---|---|
| | | | • monitoring.<br>• The efficiency of a data centre should be assessed in line with Recommendations ITU T L.1400, ITU T L.1410 and ITU T L.1420. | |
| **4** | ITU-T SG5 | **L.1310**<br>Energy efficiency metrics and measurement methods for telecommunication equipment | This Recommendation contains the definition of energy efficiency metrics test procedures, methodologies and measurement profiles required to assess the energy efficiency of telecommunication equipment.<br>Energy efficiency metrics and measurement methods are defined for telecommunication network equipment and small networking equipment.<br>These metrics allow for the comparison of equipment within the same class, e.g., equipment using the same technologies. | Published (08/2014) |
| **5** | ITU-T SG5 | **L.1320**<br>Energy efficiency metrics and measurement for power and cooling equipment for telecommunications and data centres | This Recommendation contains the general definition of metrics, test procedures, methodologies and measurement profiles required to assess the energy efficiency of power and cooling equipment for telecommunications and data centres. More detailed measurement procedures and specifications can be developed in future related ITU-T Recommendations.<br>Metrics and measurement methods are defined for power equipment, alternating current (AC) power feeding equipment (such as AC uninterruptible power supply (UPS), direct current (DC/AC) inverters), DC power feeding equipment (such as AC/DC rectifiers, DC/DC converters), solar equipment, wind turbine equipment and fuel cell equipment.<br>In addition, metrics and measurement methods are defined for cooling equipment such as air conditioning equipment, outdoor air cooling equipment and heat exchanging cooling equipment. | Published (03/2014) |
| **6** | ITU-T SG5 | **L.1340**<br>Informative values on the energy efficiency of telecommunication equipment | This Recommendation defines a set of informative values for telecommunication network equipment and small networking equipment used in the home and small enterprise locations. The goal is to provide useful information to support a fast deployment of energy-efficient broadband and ultra-broadband networks.<br>Such informative values refer to the metrics, test procedures, methodologies and measurement profiles that have been defined in [ITU-T L.1310]. | Published (02/2014) |
| **7** | ITU-T SG5 | **L.1400**<br>Overview and general principles of methodologies for assessing the environmental impact of information and | This Recommendation specifies:<br>• the structure of the ITU-T L.1400-series of Recommendations, methodology of environmental impact assessment of ICT;<br>• general principles of methodology among Recommendations regarding the environmental impact assessment of ICT;<br>• mention of relevant methodologies in other SDOs;<br>• presentation of each Recommendation from the future ITU-T L.1400-series Recommendations on methodology. | Published (02/2011) |

| | | | | |
|---|---|---|---|---|
| | | communication technologies | This Recommendation refers to documents that are being considered for preparation in the area of general principles of methodologies for assessing the environmental impact of ICTs. The specific designation of these documents (marked by *) will be indicated once approved for publication. | |
| **8** | ITU-T SG5 | **L.1500** Framework for information and communication technologies (ICTs) and adaptation to the effects of climate change | This ITU-T Recommendation describes the framework for using ICTs in adaptation to the effects of climate change. This Recommendation will define the scope of the subsequent three Recommendations to be published within this framework.<br>This Recommendation does not provide strategies or best practices for climate change adaptation as these will be provided in the Recommendations developed within this framework. | Published (06/2014) |
| **9** | ITU-T SG13 | **Y.2070** Requirements and architecture of home energy management system and home network services | This ITU-T Recommendation ) provides the requirements and architecture of home energy management system (HEMS) and home network (HN) services | Published (01/2015) |
| **10** | ITU-T SG13 | **Y.2064** Energy saving using smart objects in home networks | This ITU-T Recommendation describes requirements and capabilities for saving energy by using smart objects in home networks. It also presents the functional architecture of key components for saving energy through home/building automation. | Published (01/2014) |
| **11** | ITU-T SG13 | **Y.2200-series** Greenhouse gas monitoring services provided over NGN | This supplement describes general aspects of the GHG monitoring issue, and it provides requirements and required functions. In addition, a service model and functional architecture for a GHG monitoring service are presented. NGN-based GHG monitoring service scenarios are also presented | Published (06/2013) |
| **12** | ITU-T SG13 | **Y.meg** | This draft Recommendation provides the framework of micro energy grid for interconnected local generation and distribution. After identifying key features from the concepts of micro energy grid, this draft Recommendation specifies requirements and capabilities in terms of networks and services as well as users considering distributed energy sources. Then, this draft Recommendation provides architectural overview including the domain model as well as the functional architecture and deployment models. Finally detailed operations of control and management services for micro energy gird are described. | Under Study |
| **13** | ITU-T SG13 | **Y.sfem-WoO** | This draft Recommendation identifies the service framework of Web of Objects (WoO) for management for energy/power consumption, measurement and efficiency. The service | Under Study |

| | | | | |
|---|---|---|---|---|
| | | | framework of WoO for energy efficiency management is defined by considering energy efficiency management model, requirements, the architectural interactive model between user web service and server /repository in auto-identified objects in the home, building, and Under Study factory. | |
| **14** | ITU-T SG13 | **Y.energyECN** | This draft Recommendation describes the energy efficiency class of networks, taking into account the requirements, the definition of the energy efficiency classes. It also guides the applications including examples and required candidate technologies for each energy efficiency class. The main objective of this Recommendation is to recommend using appropriate network equipment to certain networks by energy efficiency class. | Under Study |
| **15** | ITU-T SG13 | **Y.energy-plataform** | This draft Recommendation provides the framework of energy sharing and trading platform for integrated control and management considering energy producing, storing and consumption. After identifying key characteristics and core technologies of the platform, this draft Recommendation specifies requirements taking into account the energy value chain comprising various stakeholders. Then, this draft Recommendation provides architectural overview specifying related interfaces and functional blocks. Finally mechanisms for energy information exchange and detailed operations of integrated control and management services on the energy sharing and trading platform are described | Under Study |
| **16** | FG-SSC | **FG-SSC** Deliverable Overview and Role of ICT in Smart Sustainable Cities | The goal of this report is to provide an overview of a smart sustainable city and establish what the role of ICT is in relation to such an urban environment. The approach taken by this team, as part of the FGSSC Working Group 1 was to first establish the different indicators, parameters which define a smart sustainable city and ensure that these are drawn from as wide a variety of sources and perspectives as possible. Such an approach ensured that the results were balanced and not skewed towards one stakeholder or other. | Under Study |
| **17** | FG-SSC | **FG-SSC** Deliverable Smart Sustainable Cities Infrastructure | The goal of this report is to provide a technical overview on infrastructure related to information and communications technology (ICT) and specifically, to develop a smart sustainable city (SSC). This document is divided into five sections. | Under Study |
| **18** | FG-SSC | **FG-SSC** Deliverable ICTs for Climate Change Adaptation in Cities | This technical report has been developed within the Focus Group on Smart Sustainable Cities and responds to the need of exploring how Information and Communication Technologies (ICTs) and its infrastructure can support cities' adaptation to climate change. This technical report has been also developed with the aim of contributing to the ongoing work on climate change adaptation within Question 15/5 of ITU-T Study Group 5, which leads ITU-T standardization activities on ICT environmental aspects of climate change. | Under Study |
| **19** | FG-SSC | **FG-SSC** Deliverable | From inception Information and Communication Technologies (ICTs) have played a pivotal role in the lives of cities. Historically cities have been generating economic growth of countries by developing institutions and assembling human resource to achieve prosperity, | Under Study |

| | | | | |
|---|---|---|---|---|
| | | Smart Water Management in Cities | unfortunately at a cost of its water resource. With urbanization becoming an inevitable truth, cities are enduring more and more challenges to secure financially sustainable water and sanitation services for it citizenry. If matched with appropriate and effective Information and Communication Technologies (ICTs), in the form of Smart Water Management (SWM), water issues within cities can be properly addressed and managed. | |
| **20** | FG-SSC | **FG-SSC** Deliverable Integrated Management for Smart Sustainable Cities | By promoting the coordinated development and management of smart sustainable cities, Integrated Management for Smart Sustainable Cities allows cities to maximize socioeconomic institutions as well as keep the city operate in an orderly way. However, in order to realize the orderly operation of all relevant sectors in the cities, a series of technical specification is essential. Thus this Technical Report aspires to emphasize the management problems faced in cities and pose Integrated Management for Smart Sustainable Cities as a possible solution to mitigate such challenges, with the main intent to generate further dialogue and discussion. | Under Study |

## 5. Convergences over broadband networks

### 5.1 IPTV

#### 5.1.1. Overview

IPTV is defined as multimedia services such as television/video/audio/text/graphics/data delivered over IP-based networks managed to support the required level of QoS/QoE, security, interactivity and reliability. The definition of IPTV services encompasses not only simple TV services but also services that involve a combination of communication and video delivery, such as interactive advertising, video telephony, and email services. Among the wide variety of IPTV services, studies target the provision of IPTV basic services in the form of linear TV (ordinary broadcast-type services) and video on demand (VoD)[128].

Figure 5-1-1 shows the main domains that are involved in the provision of an IPTV service. These domains do not define a business model[129]. The following definition can be used:

- Content provider: The entity that owns or is licensed to sell content or content assets.
- Service provider A general reference to an operator that provides telecommunication services to customers and other users either on a tariff or contract basis. A service provider can optionally operate a network. A service provider can optionally be a customer of another service provider.
- Network provider: The organization that maintains and operates the network components required for IPTV functionality.
  NOTE – Although considered as two separate entities, the service provider and the network provider can optionally be one organizational entity.
- End user: The actual user of the products or services.

.

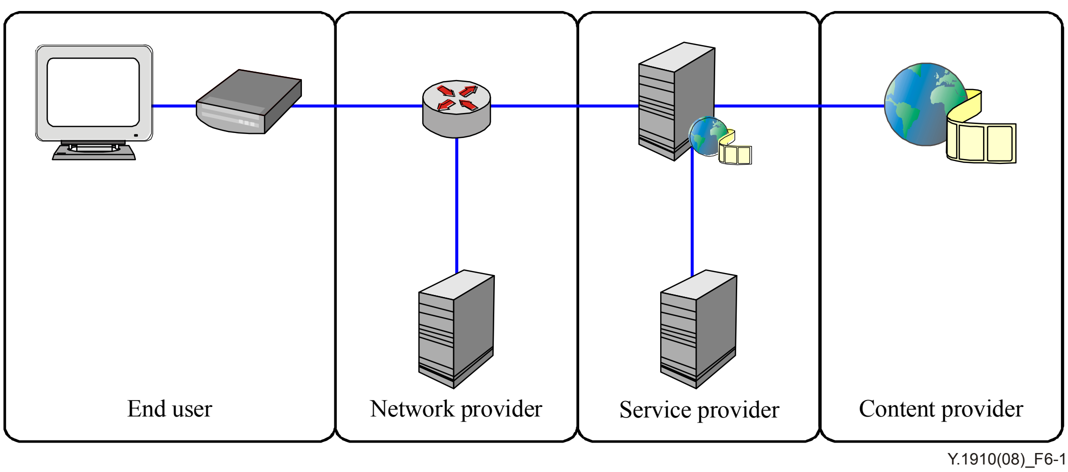



Figure 5-1-1 IPTV domains

[128] ITU Academy – IPTV training course: https://academy.itu.int/news/item/328-iptv

[129] ITU-T Recommendation Y.1910, "IPTV functional architecture," 2008.

- **Installation, terminal devices and functional component Options**

Different installation options are available for each IPTV domain. The Chapter 3 of this Report dedicates itself for presenting different infrastructure solutions. Besides, ITU-T H.720 gives an overview of Internet Protocol television (IPTV) terminal devices and end systems presenting the Figure 5-1-2 that are implemented by different vendors.

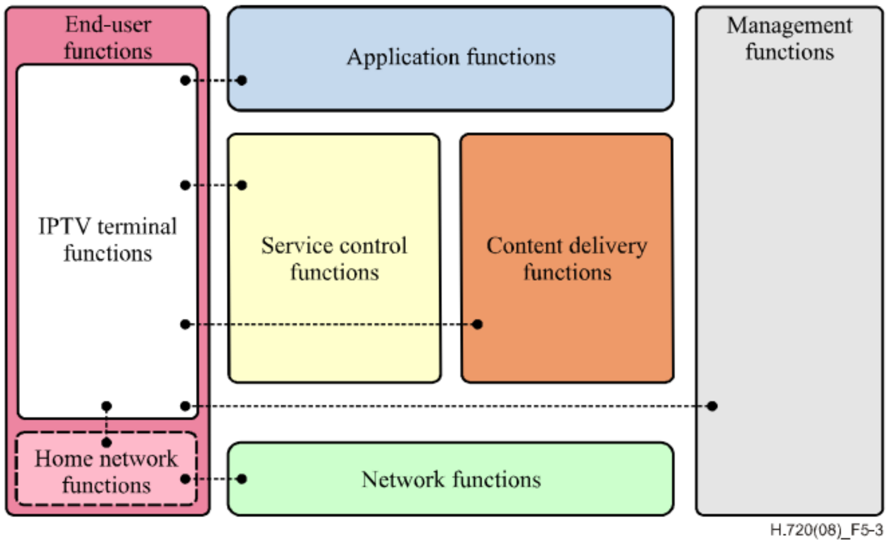



Figure 5-1-2 – IPTV terminal device architectural overview

A comparison between terminals and systems solutions is brought by Chapter 6.5 of this Report.

### 5.1.2. Required Capabilities for IPTV

- **Core Network Consideration for IPTV Deployment**[130]
- The IPTV architecture is required to allow for a two-way communication between the end-user and the service provider.
- The IPTV architecture is required to support mechanisms to support on demand services.
- The IPTV architecture is required to support a means for the service provider to provide an integrated presentation of content received at the IPTV terminal via out-of-band delivery methods and via IP networks.
- The IPTV architecture is required to support capabilities for management of capacity on service and network elements.
- The IPTV architecture is required to support multicast means of communication to all end-users.
- The IPTV architecture is recommended to support Ipv4 and Ipv6.
- The IPTV architecture is recommended to support the download of content regardless of its type, e.g., audio, video, text, graphics.
- The IPTV architecture is recommended to support both a pull and a push method of content delivery.
- The IPTV architecture is recommended to present an open interface for 3rd party applications to use the capabilities and resources of the service and network functional components.
- The IPTV architecture is recommended to support mechanisms that allow IPTV services to be distributed to specific groups of end-users.

- **Home/Access Network Consideration for IPTV Deployment**

130 ITU-T Recommendation Y.1901, "Requirements for the support of IPTV services," 2009.

- The IPTV architecture is required to support a mechanism for NAT traversal.
- The IPTV architecture is recommended to allow the delivery of IPTV services over different access networks.
- The IPTV architecture is recommended to support both static and dynamic address allocation, numbering and naming schemes.
- The IPTV architecture can optionally support content sharing between devices in the home network.

- **QoS/QoE Consideration for IPTV Deployment**
- The network that supports IPTV is required to support IP QoS classes and to satisfy associated performance requirements specified in [ITU-T Y.1541].
- The IPTV architecture is required to support a mechanism for assigning IPTV traffic priorities.
- The IPTV architecture is required to support a mechanism that allows for service-based transport QoS to be managed across multiple network provider domains.
- The IPTV architecture is required to support a framework that identifies the components and measurement points for QoS measurement.
- The IPTV architecture is required to allow the delivery of IPTV services with defined QoE for the IPTV end-user.
- The IPTV architecture is recommended to rely upon any relevant QoS capabilities when integrating IPTV services into NGN-based environments.
- The IPTV architecture is recommended to support capabilities to monitor audio and video quality.

- **IPTV Mobility Consideration**
- The IPTV architecture is required to support nomadism for both personal mobility and terminal mobility.
- The IPTV architecture is recommended to support functions in order to adapt dynamically to changes in wireless networks characteristics when the service is delivered over a mobile network, e.g., bandwidth, packet loss rate.
- The IPTV architecture is recommended to allow seamless IPTV service provision and operation across different networks supporting IPTV services.

### 5.1.3. Role and Key Areas of ICT infrastructure for IPTV

- **IPTV Architectural Approaches**[131]

There are three IPTV architecture approaches that enable service providers to deliver IPTV services:

- "Non-NGN IPTV functional architecture" (non-NGN IPTV): The non-NGN IPTV architecture is based on existing network components and protocols/interfaces. The technology components, protocols and interfaces used in this IPTV architecture are already in use and hence this approach is a representation of typical existing networks providing IPTV services.
- "NGN-based non-IMS IPTV functional architecture" (NGN non-IMS IPTV): The NGN non-IMS IPTV architecture utilizes components of the NGN framework reference architecture as identified in [ITU-T Y.2012] to support the provision of IPTV services, in conjunction with other NGN services if required.
- "NGN IMS-based IPTV functional architecture" (NGN-IMS IPTV): The NGN IMS-based IPTV architecture utilizes components of the NGN architecture including the IMS component to support the provision of IPTV services in conjunction with other IMS services if required.

The NGN-based IPTV architecture is based on the NGN architecture defined in [ITU-T Y.2012] and uses the components and functions of the NGN. The non-NGN-based IPTV architecture does not necessarily require these components and functions and uses conventional and/or legacy network technologies for the delivery of IPTV services. The main differences are described below:

---

[131] ITU-T Recommendation Y.1910, "IPTV functional architecture," 2008.

- The NGN-based IPTV architecture uses network attachment control functions (NACF) defined in [ITU-T Y.2014] to provide functions such as authentication and IP configuration.
- The NGN-based IPTV architecture uses resource and admission control functions (RACF) defined in [ITU-T Y.2111] to provide resource and admission control functions.
- The NGN-based IPTV architecture uses service control functions defined in [ITU-T Y.2012] to provide service control functions.

The NGN-IMS-based IPTV architecture uses core IMS functions and associated functions such as the service user profile functional block defined in [ITU-T Y.2021] to provide service control functions. The NGN non-IMS-based IPTV architecture uses service control functions other than core IMS functions to provide service control functions.

### 5.1.4. IPTV Architectural Overview

Figure 5-1-3 provides an overview of the IPTV functional architecture[132].

- End-user Functions

The end-user functions are comprised of IPTV terminal functions and home network functions.

- IPTV terminal functions: The IPTV terminal functions (ITF) are responsible for collecting control commands from the end user and interacting with the application functions to obtain service information (e.g., Electronic program guides (EPG)), content licenses and keys for decryption. They interact with the service control and content delivery functions to receive the IPTV services and also provide the capability for content reception, decryption and decoding.
- Home network functions: The home network functions provide the connectivity between the external network and each IPTV terminal device. These functions include IP connectivity, IP address allocation and configuration from the network functions to the IPTV terminal devices. All data, content and control traffic must pass through the home network functions in order to enter or exit the end-user's IPTV terminal device.

- Application Functions
- IPTV application functions: The IPTV application functions enable the IPTV terminal functions to select and purchase, if necessary, content. When receiving requests from IPTV terminal functions, the IPTV application functions perform application authorization and execution of IPTV service logic.
- Application profile functional block: The IPTV application profile can optionally include end-user settings, global settings, linear TV settings, list of subscribed linear TV service packages, VoD settings, etc.
- Content preparation functions: The content preparation functions control the preparation and aggregation of the contents such as VoD programme, TV channel streams, metadata and EPG data.
- Service and content protection (SCP) functions: The SCP functions control the protection of the services and content. Content protection includes control of access to contents and the protection of contents using methods such as encryption.

- Service Control Functions
- IPTV service control functional block: The IPTV service control functional block provides the functions to handle service initiation, modification and termination requests, perform service access control, establish and maintain the network and system resources required to support the IPTV services requested by the IPTV terminal functions.
- Service user profile functional block: The service user profile functional block store end-user service profile, subscriber-related data, end-user location data, end-user presence status, etc.

- Content Delivery Functions
- The content delivery functions (CDF) perform cache and storage functionalities and deliver the content according to the request from the end-user functions.

---

[132] ITU-T Recommendation Y.1910, “IPTV functional architecture,” 2008.

- Multiple instances of storage and delivery functionalities can optionally exist. The content delivery functions select the suitable one(s). To maintain the same content at the multiple instances, the content delivery functions control the distribution of content to multiple instances of storage and delivery functionalities.
- Content distribution and location control functions: The content distribution and location control functions handle interactions with the IPTV service control functional block, control the distribution of content from the content preparation functions to the content delivery and storage functions and perform the selection of suitable content delivery and storage functions to serve end-user functions according to certain criteria.
- Content delivery and storage functions: The content delivery and storage functions store and cache the content, process it under the control of content preparation functions and distribute it among instances of content delivery and storage functions based on the policy of content distribution and location control functions.

- Network Functions
- The network functions are shared across all services delivered by IP to end-user functions. The network functions provide the IP layer connectivity to support IPTV services.
- Authentication and IP allocation functional block: The authentication and IP allocation functional block provides the functionality to authenticate the delivery network gateway functional block which connects to the network functions, as well as allocation of IP addresses to the delivery network gateway functional block.
- Resource control functional block: The resource control functional block provides control of the resources which have been allocated for the delivery of the IPTV services through the access network, edge and core transport functions.
- Transport functions: The transport functions provide IP layer connectivity between the content delivery functions and the end-user functions. The transport functions include access network functions, edge functions, core transport functions and gateway functions.
- Access network functions: Access network functions are responsible for: 1) aggregating and forwarding the IPTV traffic sent by the end-user functions into the edge of the core network: and 2) forwarding the IPTV traffic from the edge of the core network towards the end-user functions.
- Edge Functions: Edge functions are responsible for forwarding the IPTV traffic aggregated by the access network functions towards the core network, and also to forward the IPTV traffic from the core network to the access network functions.
- Core transport functions: Core transport functions are responsible for forwarding IPTV traffic throughout the core network.

- Management Functions
- The management functions handle overall system status monitoring and configuration. This set of functions can optionally be deployed in a centralized or a distributed manner.
- Management functions are comprised of application management functional block, content delivery management functional block, service control management functional block, end-user device management functional block, and transport management functional block.

- Content Provider Functions
- Content provider functions provide the content and associated metadata to content preparation functions, which contain the following sources.
- Content and metadata sources: The content and metadata sources include content protection rights sources, content sources and metadata sources for the IPTV services.

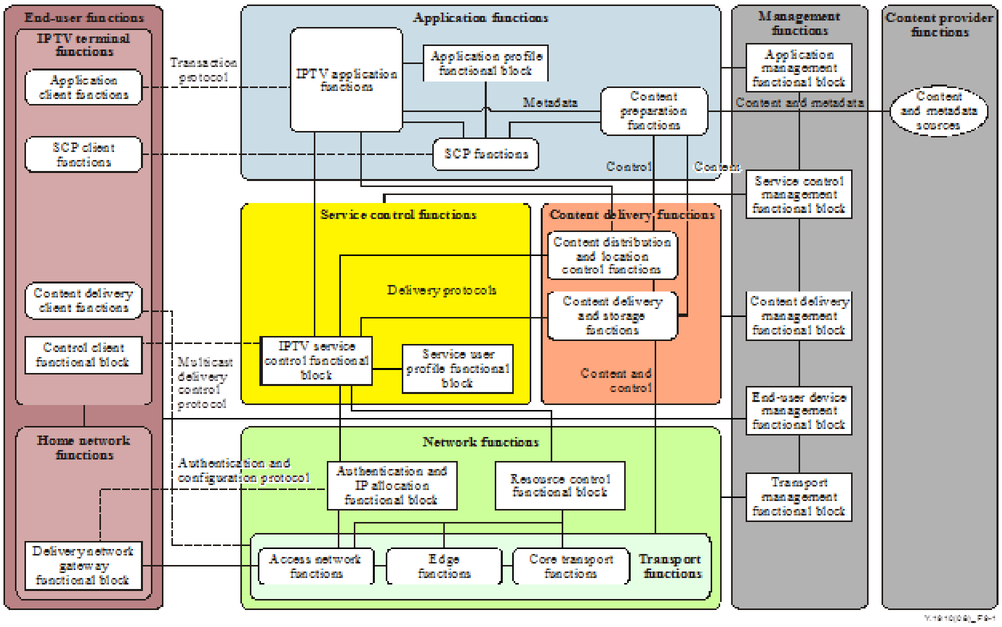



Figure 5-1-3 IPTV architectural overview[133]

## 5.1.5. Standardization for IPTV

The ITU-T IPTV Global Standards Initiative[134] organizes events for the development of ITU-T Recommendations for IPTV, where Questions from relevant study groups meet together to efficiently develop IPTV standards[135].

---

133 ITU-T Recommendation Y.1910, "IPTV functional architecture," 2008.

134 SG 16 is the parent ITU-T Study Group of the IPTV GSI. A roadmap for IPTV related Recommendation is available at http://www.itu.int/en/ITU-T/studygroups/2013-2016/16/Pages/rm/iptv.aspx

135 For more information on the ITU-T IPTV GSI: http://www.itu.int/en/ITU-T/gsi/iptv/Pages/default.aspx

- ITU related Documents

| No | Group | Document title | Scope of document | Status |
|---|---|---|---|---|
| **1** | ITU-T SG9 | **J.700** IPTV service requirements and framework for secondary distribution | This Recommendation describes the service requirements and functional framework architecture for support of IPTV services to provide enhanced broadcasting. It addresses the service requirements, use cases and functional components required to support these requirements. Where possible, this Recommendation utilizes the material already developed, or under development, in ITU-T Recommendations related to video service delivery over secondary networks. | Published (12/2009) |
| **2** | ITU-T SG9 | **J.701** Broadcast-centric IPTV Terminal middleware | This Recommendation defines components of a broadcast-centric IPTV terminal middleware and provides a high-level description of functionality necessary to support IPTV services. These definitions and descriptions are intended to assist in the establishment of a migration path to meet immediate market demand to deploy IPTV services. | Published (10/2008) |
| **3** | ITU-T SG9 | **J.702** Enablement of current terminal devices for the support of IPTV services | This Recommendation describes an IPTV terminal device that enables a migration path for the support of basic IPTV services for current terminal devices used for other TV delivery services. This document identifies architectures and functions needed for the IPTV terminal to support basic IPTV services, and is intended to meet immediate demands of current TV delivery services. | Published (10/2008) |
| **4** | ITU-T SG9 | **J.703** IPTV Client Control Interface Definition | The scope of this Recommendation is the i-3 interface, identified as control interface for IP transport for enhanced broadcasting defined in J.700. Examples of content and application to be requested through the i-3 interface include digital video and audio program content, including the metadata describing the program content, and applications to be presented or executed at the Service Client. | Published (3/2010) |
| **5** | ITU-T SG9 | **J.705** IPTV client provisioning, activation, configuration and management Interface Definition | The scope of this Recommendation is the i-2 interface which enables the Service Client in the Customer Network to interface with the OSS Functions in the Operator Network to provision and manage the IPTV Client functions in the Customer Network. | Published (1/2011) |
| **6** | ITU-T SG9 Q.8 | **J.iptvappclient** Description of the Application Client Interface | The scope of this Recommendation is the i-6 interface, identified in J.700, which enables application functions of the operator network and the application client of the customer network to interface in such a way that the provisioning and functionality of applications are managed appropriately. | Under study |
| **7** | ITU-T SG9 Q.8 | **J.iptvcontentclient** Description of the IPTV Content Client Interface | The scope of this recommendation is the i-4 interface, identified in J.700, which enables the Operator Network IPTV Content Functions to send real-time digital video and audio media and associated metadata over IP to the Content Client in the Customer Network. | Under study |
| **8** | ITU-T SG11 | **Q.3040** Signalling and control plane architecture for IPTV | This Recommendation describes the overall signalling architecture for IPTV control plane. It identifies the functions, functional blocks, physical entities, interfaces, and protocols that will model the control plane for IPTV. | Published (8/2010) |

| | | | | |
|---|---|---|---|---|
| **9** | ITU-T SG11 | **X.604.2** Information technology - Mobile multicast communications: Protocol over overlay multicast networks | This Recommendation describes an application-level protocol that supports relayed multicast data transport capability over the IP-based wireless networks as well as the wired fixed networks. This protocol focuses on one-to-many data delivery service types. | Published (10/2010) |
| **10** | ITU-T SG12 | **G.1080** Quality of experience requirements for IPTV services | This Recommendation defines user requirements for Quality of Experience (QoE) for IPTV services. The QoE requirements are defined from an end-user perspective and are agnostic to network deployment architectures and transport protocols. The QoE requirements are specified for the end-to-end service and information is provided on how they influence network transport and application layer behaviour. | Published (12/2008) |
| **11** | ITU-T SG12 | **G.1081** Performance monitoring points for IPTV | This Recommendation defines performance monitoring points for IPTV which will allow the service provider/network operator to monitor the performance of the complete IPTV service delivery to the end user. Successful deployment of IPTV services requires performance to be monitored at the customer set-top-box and at interconnect points between disparate network domains. | Published (10/2008) |
| **12** | ITU-T SG12 | **G.1082** Measurement-based methods for improving the robustness of IPTV performance | This Recommendation describes some methods by which measurement information of IPTV service quality can be used to dynamically control the performance of an IPTV service such as network resource allocation, FEC redundant encoding, delivery path selection or media encoding bit rate if scalable encoding is employed. | Published (4/2009) |
| **13** | ITU-T SG13 | **Y.1901** Requirements for the support of IPTV services | This Recommendation specifies the high level requirements to support IPTV services. These include IPTV requirements for service offering, network aspects, QoS and QoE, service and content protection, end system, middleware and content. | Published (01/2009) |
| **14** | ITU-T SG13 | **Y.1902** Framework for multicast-based IPTV content delivery | This Recommendation provides a framework for multicast-based IPTV content delivery based upon different content delivery functional models and their associated requirements for delivery of IPTV content to multiple end users simultaneously. | Published (04/2011) |
| **15** | ITU-T SG13 | **Y.1903** Functional requirements of mobile IPTV | This Recommendation describes detailed functional requirements of mobile IPTV, which is an application of IPTV. It applies to where the IPTV terminal device is connected to the IPTV service provider via an IPTV-enabled mobile network to provide the IPTV services irrespective of changes of the location or technical environment. | Published (01/2014) |
| **16** | ITU-T SG13 | **Y.1910** IPTV functional architecture | This Recommendation describes the IPTV functional architecture intended to support IPTV services based on the IPTV service requirements and definitions. Starting from a basic description of IPTV roles and services, a high level IPTV functional model is outlined. This model is then developed into a more detailed functional architecture. | Published (09/2008) |
| **17** | ITU-T SG13 | **Y.1911** IPTV services and nomadism: Scenarios and functional architecture for unicast delivery | This Recommendation describes scenarios for the support of IPTV services to nomadic end users taking into account the requirements identified in [ITU-T Y.1901] and the functional architecture defined in [ITU-T Y.1910]. This Recommendation also describes functional architectures, reference points and information flows based on the scenarios identified in this Recommendation. | Published (04/2010) |

| | | | | |
|---|---|---|---|---|
| **18** | ITU-T SG13 | **Y.1920**<br>Guidelines for the use of traffic management mechanisms in support of IPTV services | This Recommendation defines functional requirements which are derived from the high-level requirements of traffic mechanisms in [ITU-T Y.1901]. Based on them, a set of traffic management mechanisms at the transport stratum in support of IPTV services are described from the perspectives of control plane, data plane and management plane. Guidelines on how such mechanisms can be used to effectively meet the functional requirements are also provided in detail. | Published (07/2012) |
| **19** | ITU-T SG13 | **Y.1991**<br>Terms and definitions for IPTV | This Recommendation contains terms and definitions and a framework relevant to providing a general understanding of IPTV. This Recommendation is not simply a compendium of terms and definitions. The primary purpose of this Recommendation is to provide a context for the use of certain terms and definitions to avoid misunderstandings in IPTV and IPTV-related activities. | Published (03/2010) |
| **20** | ITU-T SG13 | **Y.2019**<br>Content Delivery and Storage Architecture in NGN | This Recommendation specifies the functional architecture of content delivery functions in NGN and the related procedures. This Recommendation builds upon the IPTV functional architecture described in [ITU-T Y.1910]. | Published (9/2010) |
| **21** | ITU-T SG13 | **Y.Suppl. 5**<br>ITU-T Y.1900-series, Supplement on IPTV service use cases | The IPTV Service Use Cases document provides a list of IPTV use cases that are informative illustrations of how IPTV services can be designed, deployed and operated. From the end-user's perspective, use cases have been categorized by distributed content services, interactive services, communication services, and others. | Published (5/2008) |
| **22** | ITU-T SG13 | **Y.Suppl.16**<br>ITU-T Y.1900-series - Guidelines on deployment of IP multicast for IPTV content delivery | This Supplement describes the technical guidelines for the deployment of IP multicast technologies for IPTV content delivery. The deployment guidelines identify the technical issues and considerations regarding the capabilities of IP multicast from the perspective of supporting the IPTV services.<br>This Supplement can be used for IPTV content delivery using the network multicast-based content delivery model defined in [ITU-T Y.2019] and [ITU-T Y.1902]. | Published (2/2012) |
| **23** | ITU-T SG13 | **Y.Suppl.20**<br>Scenarios and use cases of mobile IPTV | This Supplement provides mobile IPTV use cases as informative illustrations of how mobile IPTV services can be designed, deployed, and operated. The use cases are described with sample scenarios and operational procedures of mobile IPTV services. In addition, the use cases detail functional procedures to illustrate how the service scenarios can be supported with IPTV architectural functions. | Published (6/2012) |
| **27** | ITU-T SG16 | **H.622.1**<br>Architecture and functional requirements for home network supporting IPTV services | This Recommendation describes relationship between the home network and IPTV related entities. It also identifies rules and requirements for functions needed on the home network to support IPTV services. It further sets criteria to verify compliance of home network devices, e.g. IPTV terminal devices, to the identified rules and requirements. | Published (10/2008) |
| **28** | ITU-T SG16 | **H.701**<br>Content Delivery Error Recovery for IPTV services | The ability to deliver high level of service quality to users is an essential aspect of IPTV services, and thus captured in many IPTV-related requirements. As IPTV services can easily be degraded if the media decoders are exposed to impairments such as packet losses, mechanisms are needed to reliably deliver good IPTV service quality in the presence of such defects. | Published (3/2009) |
| **29** | ITU-T SG16 | **H.702**<br>Accessibility profiles for IPTV systems | This Recommendation defines three profiles for accessibility features in IPTV systems, with increasing levels of support. While the Basic Profile provides an entry-level support of accessibility, the Main Profile provides the widest range of features; the Enhanced Profile provides the middle level support between the Basic Profile and the Main Profile. Accessibility information is information such as captions, sign language streams and audio description that are sent separately | Approved (11/2015) |

| | | | | |
|---|---|---|---|---|
| | | | from video contents to IPTV terminal devices. By defining the above profiles, persons with disabilities can choose more easily the terminal devices that have the functions they need. | |
| **30** | ITU-T SG16 | **H.720** Overview of IPTV terminal devices and end systems | This Recommendation gives the overview of IPTV terminal device and end systems. It also gives general architecture and functional components of an IPTV terminal device, providing a high-level description of functionality of terminal devices for IPTV services. | Published (10/2008) |
| **31** | ITU-T SG16 | **H.721** IPTV Terminal Device: Basic model | This Recommendation describes and specifies the functionalities of the IPTV terminal devices for IPTV basic services defined in [ITU-T H.720], over a dedicated content delivery network, which takes into consideration such conditions on content delivery as QoS. | Published (3/2009) |
| **32** | ITU-T SG16 | **H.722** IPTV terminal device: Full-fledged model | Recommendation ITU-T H.722 describes the services and key features of the full-fledged Internet Protocol TV terminal device (IPTV TD) defined in Recommendation ITU-T H.720. In comparison with the IPTV TD-basic model defined in Recommendation ITU-T H.721, the full-fledged IPTV TD supports not only such basic services as linear TV and video-on-demand (VoD), but also advanced services such as Internet, medical applications, communications, etc. Based on these services and key features, this Recommendation specifies the architecture of the full-fledged IPTV TD, functional components within its architecture, software architecture for implementation reference and physical interfaces | Approved (2014-01) |
| **33** | ITU-T SG16 | **H.730** Web-based terminal middleware for IPTV services | This Recommendation defines web-based terminal middleware, its general architecture, and interfaces as required by IPTV services. This Recommendation is based on the ITU-T H.720 series for the specifications of IPTV terminal devices and the ITU-T H.760 series for multimedia interactivity and web-related technologies. | Published (6/2012) |
| **34** | ITU-T SG16 | **H.740** Application event handling for IPTV services | This Recommendation provides a framework of application event handling for IPTV. A specific user interaction or occurrence related with multimedia content in IPTV can be called an application event. This Recommendation describes general aspects for IPTV application event services, such as emergency alert and audience measurement. | Published (3/2010) |
| **35** | ITU-T SG16 | **H.741.x** IPTV application event handling: Audience measurement | The ITU-T H.741.x series of Recommendations defines a foundational platform for audience measurement (AM) of IPTV services. They focus on the interface between terminal devices and an audience measurement aggregation function. The design philosophy in the ITU-T H.741.x series is focused on scalability, minimizing the use of resources, security, flexibility to support a variety of service provider deployments, and rich privacy support to meet emerging regulations and legislation.<br><br>The AM platform integrates a method for end users to report personal information, and is designed to easily add time-shifted and interactive services, and non-terminal device measurement points. While the ITU-T H.741.x series allows the implementation of audience measurement for IPTV services, its mechanism may be equally applicable to non-IPTV services.<br><br>Recommendation ITU-T H.741.0 defines a foundational platform for audience measurement (AM) of Internet Protocol television (IPTV) services. This Recommendation focuses on the interface between terminal devices (TDs) and an audience measurement aggregation function. The AM platform integrates a method for end users to report personal information, and is designed to easily add time-shifted and interactive services, and non-terminal device measurement points. While ITU-T H.741.0 allows the implementation of audience measurement for IPTV services, its mechanism may be equally applicable to non-IPTV services. The audience measurement mechanism specified in H.741.0 provides additional benefits when compared to traditional audience measurement. Such benefits include, in particular, a larger audience population sample, more detailed engagement metrics, passive data collection, and feedback for the enhancement of services. The | Published (2012) |

| | | | | |
|---|---|---|---|---|
| | | | AM platform integrates a method for end users to report personal information, and is designed to easily add time-shifted and interactive services, and non-terminal device measurement points. While the ITU-T H.741.x series allows the implementation of audience measurement for IPTV services, its mechanism may be equally applicable to non-IPTV services.<br><br>Recommendation ITU-T H.741.1 specifies the operations of AM, including procedures prior to configuration of terminals, configuration of terminals, reporting by terminals, security mechanisms, and recovery from abnormal situations. Informative Appendices I-VII discuss discovery metadata, implementation considerations, examples, permission levels, vendor considerations, alternative privacy schemes, and discuss capabilities and profiles.<br><br>Recommendation ITU-T H.741.2 specifies the data elements and structures of the payloads used in audience measurement messages.<br><br>Recommendation ITU-T H.741.3 specifies audience measurement for IPTV distributed content services and, in particular, linear TV services. It describes specific configuration for linear TV and metadata and data structures used in the payload of AM messages. The informative appendices discuss specific implementation considerations for linear TV-specific implementation considerations, provide examples and describe capabilities and profiles.<br><br>Recommendation ITU-T H.741.4 specifies the data elements and structures of the transport delivery-dependent XML and binary headers, used in audience measurement messages. Appendix I provides an analysis of AM to understand its transport protocol requirements. | |
| **36** | ITU-T SG16 | **H.750**<br>High-level specification of metadata for IPTV services | This Recommendation gives the high-level specification of the metadata for IPTV services, its elements, and delivery protocols. The IPTV metadata provides a descriptive and structural framework for managing IPTV services. The IPTV metadata is the information on services and contents processed by service and content delivery infrastructure. | Published (10/2008) |
| **37** | ITU-T SG16 | **H.751**<br>Metadata for rights information interoperability in IPTV services | This Recommendation gives the high-level specification of the metadata for rights information interoperability, including representation of the minimum required elements. The rights information interoperability metadata provides descriptive and contextual classification for representing rights information using the permission framework. | Published (3/2013) |
| **38** | ITU-T SG16 | **H.752**<br>Multimedia content provisioning interface for IPTV services | Recommendation ITU-T H.752 gives a description of the metadata elements that are necessary for multimedia content provisioning, such as content description, distribution conditions and usage log report. Comparing with the high-level specification of metadata for IPTV services defined in Recommendation ITU-T H.750, multimedia content provisioning interface for IPTV services focuses on the metadata elements to be used at the interface between content providers and IPTV service providers. This Recommendation specifies the requirement for AV content metadata provisioning, AV content metadata elements and data structure, procedure of exchanges for content between the content providers and IPTV service providers. | Approved (11/2015) |
| **39** | ITU-T SG16 | **H.760** | This Recommendation identifies and describes the relevant standards for interoperability and harmonization among IPTV multimedia application frameworks. | Published (3/2009) |

| | | | | |
|---|---|---|---|---|
| | | Overview of Multimedia Application Frameworks for IPTV | | |
| **40** | ITU-T SG16 | **H.761** Nested Context Language (NCL) and Ginga-NCL for IPTV services | This Recommendation specifies the Nested Context Language (NCL) and an NCL presentation engine called Ginga-NCL to provide interoperability and harmonization among IPTV multimedia application frameworks. To provide global standard IPTV services, it is foreseeable that a combination of different standard multimedia application frameworks will be used. Therefore, this Recommendation specifies the Nested Context Language to provide interoperable use of IPTV services. | Published (4/2009) |
| **41** | ITU-T SG16 | **H.762** Lightweight interactive multimedia environment (LIME) for IPTV services | This Recommendation describes the high-level functionalities of the lightweight interactive multimedia framework (LIME) for IPTV. LIME supports functionalities in IPTV terminal devices to provide interactivity and a variety of content such as audio, video, graphics and text. Expected services include additional data such as text to enrich TV programmes, and two-way portal pages. | Published (5/2011) |
| **42** | ITU-T SG16 | **H.763.1** Cascading style sheets for IPTV services | This Recommendation describes Cascading Style Sheets to provide interoperability and harmonization among IPTV multimedia application frameworks. To provide global standard IPTV services, it is foreseeable that a combination of different standard multimedia application frameworks will be used. | Published (9/2010) |
| **43** | ITU-T SG16 | **H.764** IPTV service enhanced script language | This Recommendation describes a script language for IPTV service, which is called IPTV SESL, to provide interoperability and harmonization among IPTV multimedia application frameworks. | Published (6/2012) |
| **44** | ITU-T SG16 | **H.765** Packaged IPTV application (widget) service | Packaged IPTV applications (IPTV widgets) are lightweight applications provided with a simple and easily accessible graphical user interface, that commonly provides a single functionality (e.g. calendars, feed aggregators etc.) and might stay persistently exhibited.<br><br>IPTV widgets may run on different types of IPTV terminal devices and therefore standardized technologies must be supported by the Widget Engine in the terminal device. This Recommendation describes IPTV widget services that are developed using the technologies defined in the ITU-T H.760 Multimedia Application Framework (MAFR) series, such as NCL (ITU-T H.761), LIME (ITU-T H.762), HTML (ITU-T H.IPTV-MAFR.13), CSS (ITU-T H.763.1), Services enhanced scripting language (ITU-T H.764) and Lua (ITU-T H.IPTV-MAFR.14). The widget service also takes advantage of functionalities described in the ITU-T H.721 IPTV terminal device basic model, as well as service discovery protocols and services specified in ITU-T H.770. | Consented (2015-02) |
| **45** | ITU-T SG16 | **H.770** Mechanisms for service discovery and selection for IPTV services | ITU-T H.770 describes the mechanisms for service provider discovery, service discovery and selection for IPTV services. The mechanisms enable IPTV terminal devices to provide the end-users with effective ways for consuming IPTV services. The expected types of IPTV services using service discovery information include Linear TV and Video-on-demand, etc. | Published (8/2009) |
| **46** | ITU-T SG16 | **H.771** SIP-based IPTV Service Discovery | This document describes the process for IPTV service provider discovery and service discovery based on SIP. The processes enable IPTV terminal device to acquire information about available IPTV service providers and IPTV services. | Published (5/2011) |
| **47** | ITU-T SG16 | **H.772** | ITU-T H.772 describes the mechanism of the IPTV terminal device discovery which makes IPTV terminal devices to be discoverable and selectable for each other within a public or local network | |

| | | | | |
|---|---|---|---|---|
| | | IPTV terminal device discovery | environment. For example, terminal device discovery is useful for services that allow users to share content to other terminal devices. The Recommendation also describes the connection model and functional architecture for IPTV terminal device functional blocks to support IPTV terminal device discovery mechanism. Moreover, the procedure of IPTV terminal device discovery is given in this Recommendation. Meanwhile, the Reference Point, the related protocols, elements and attributes to be used in the communication messages are also specified in ITU-T H.772. | |
| **48** | ITU-T SG16 | **H.780**<br>Digital signage: Service requirements and IPTV-based architecture | This draft Recommendation addresses the high level requirements, architecture and mechanisms for dealing with the aspects of digital signage contents, network, metadata and terminal devices on the basis of IPTV architecture [ITU-T Y.1910]. | Published (6/2012) |
| **49** | ITU-T SG16 | **H.781**<br>Digital Signage: Functional architecture | ITU-T H.781 defines a detailed functional architecture to provide digital signage services. The functional architecture consists of digital signage server, digital signage client, content delivery server, and content delivery client. This Recommendation describes how functions in the architecture interacts with each other to provide the services according to general information flows, and defines reference points that can be considered in specifying detailed protocols. | Consented (2015-02) |
| **50** | ITU-T SG16 | **H.785.0**<br>Digital signage: Requirements of disaster information services | This Recommendation describes overall aspects and high-level requirements for disaster information services through digital signage. The main services expected to be applied are early warning to lessen damages, reports of up-to-the-minute situations, announcements of traffic status/evacuation sites. The requirements are categorized into eight areas: general, operational management, application/delivery, contents, security, network, terminal device/display and accessibility. | Published (2014-10) |
| **51** | ITU-T SG16 | **HSTP.DS-UCIS**<br>Digital signage: Use-cases of interactive services | Digital signage (DS) is a screen media showing contents such as advertisements and notifications, which is expected to become a promising market going forward. To improve the effectiveness of notifications from users, DS services combined with interactive services have attracted attention; they also add value by providing interaction for the consumers of such services. This Technical Paper describes various use-cases of interactive DS services and explains their scenarios, functions and information flows. | Approved (2014) |
| **52** | ITU-T SG16 | **HSTP-MCTB**<br>Media coding toolbox for IPTV: Audio and video codecs | This Technical Paper contains an overview of several audio and video codecs suitable for IPTV applications. | Approved (2009) |
| **53** | ITU-T SG16 | **HSTP.CONF-H701**<br>Technical Paper: Conformance testing specification for H.701 | This Technical Paper specifies a set of attributes and procedures designed to indicate whether IPTV servers and terminal devices meet the requirements in ITU-T Rec. H.701. This set of conformance tests can provide a basic level of interoperability testing. | Published (12/2011) |
| **54** | ITU-T SG16 | **HSTP.CONF-H721 (V2)**<br>Conformance testing specification for H.721 | This Technical Paper specifies a set of attributes and procedures designed to indicate whether IPTV terminal devices meet the requirements in ITU-T Rec. H.721. This set of conformance tests can provide a basic level of interoperability testing. | Published (3/2011) |
| **55** | ITU-T SG16 | **HSTP.CONF-H761**<br>Conformance testing specification for H.761 | This Technical Paper defines the conformance testing items for ITU-T Rec. H.761 "Nested Context Language (NCL) and Ginga-NCL" as an assertion-oriented, structured specification. This approach is intended to ease the writing of testing items and to allow for the collaborative creation of H.761 test suites. | Published (5/2012) |
| **56** | ITU-T SG16 | **HSTP.CONF-H762 (V3)** | This Technical Paper defines the conformance testing items for ITU-T Rec. H.762 "Lightweight Interactive Multimedia Environment (LIME)". | Published (12/2011) |

| | | | | |
|---|---|---|---|---|
| | | Conformance testing specification for H.762 | | |
| **57** | ITU-T SG16 | **HSTP.IPTV-AISC** Technical Paper: Access to Internet-sourced contents | This Technical Paper addresses the issues related to the access to Internet-sourced contents from IPTV terminal devices. It contains the description of different configurations allowing different levels of integration of the Internet content provider catalogue and contents in the IPTV service provider environment. | Published (3/2011) |
| **58** | ITU-T SG16 | **HSTP.IPTV-ISPF** Technical Paper: IPTV retail service provider model | This Technical Paper describes IPTV retail service provider model, which is an implementation example of IPTV service provider domain. Herein, we also describe IPTV service platform as a sub-layer between eclectic mixes of service providers and network providers. | Published (7/2010) |
| **59** | ITU-T SG16 | **HSTP.IPTV-PITD** Technical Paper: Delivery and control protocols handled by IPTV terminal devices | This Technical Paper mainly describes the delivery and control protocols for IPTV terminal devices. There are several ITU-T Recommendations and well-known standards concerning IPTV services. It is therefore useful to summarize the protocols as one of overviews of standards regarding IPTV terminal devices. | Published (3/2011) |
| **60** | ITU-T SG16 | **HSTP-IPTV-AM101** Introduction to the ITU-T H.741-series - A new video engagement audience measurement standard | This Technical Paper contains an overview of the various ITU-T Recommendations dealing with IPTV audience measurement. | Published (2013) |
| **61** | ITU-T SG16 | **HSTP.IPTV-Gloss** Glossary and terminology of IP-based TV-related multimedia services | This Technical Paper contains glossary and terminology for various IPTV-related technologies. | Approved (2014) |
| **62** | ITU-T SG17 | **X.1191** Functional requirements and architecture for IPTV security aspects | This Recommendation addresses the functional requirements, architecture, and mechanisms dealing with the security and protection aspects of IPTV content, services, networks, terminal devices, and subscribers. It is anticipated that requirements and relevant functions identified in this Recommendation can be applied appropriately according to the IPTV service and business models. | Published (2/2009) |
| **63** | ITU-T SG17 | **X.1192** Functional requirements and mechanisms for the secure transcodable scheme of IPTV | This Recommendation deals with the functional requirements, architecture, and mechanisms that pertain to the security of transcoding protected IPTV content. Generic security of IPTV content is not discussed in this Recommendation. In particular, since unprotected IPTV content can be open to any user, the security of transcoding unprotected IPTV content is not discussed in this Recommendation. | Published (5/2011) |
| **64** | ITU-T SG17 | **X.1196** Framework for the downloadable service and content protection system in the mobile IPTV environment | Recommendation ITU-T X.iptvsec-6 provides a framework for the downloadable service and content protection (SCP) scheme in the mobile Internet protocol television (IPTV) environment. It also describes the functional architecture and requirements for the downloadable SCP scheme for roaming in the mobile IPTV environment. | Published (10/2012) |

| | | | | |
|---|---|---|---|---|
| **65** | ITU-T SG17 | **X.1197**<br>Guidelines on criteria for selecting cyptographic algorthms for IPTV service | Recommendation ITU-T X.iptvsec-7 provides guidelines on criteria for selecting cryptographic algorithms for IPTV service and content protection (SCP). It also provides a list of cryptographic algorithms to provide confidentiality, data origin authentication, and integrity for IPTV SCP services. | Published (4/2012) |
| **66** | ITU-T SG17 | **X.1198**<br>Virtual machine-based security platform for renewable IPTV service and content protection | This Recommendation develops a virtual machine-based security platform for renewable service and content protection (SCP) under Internet protocol television (IPTV) services. This includes the virtual machine architecture and the mechanism how to organize virtual machine-related components such as SCP client, terminal client (embedded SCP) and media client. | Published (6/2013) |

## 5.2 Cloud Computing

### 5.2.1. Overview

According to the developments of computing capabilities, users such as scientists and technologists explored ways to make large-scale computing power available to more users over time sharing, optimal use of the infrastructure, platform and prioritized access to the CPU. In addition, the ubiquitous availability of networks, low-cost computers and storage devices as well as the widespread adoption of hardware virtualization, service-oriented architecture, autonomic, and utility computing have led to growth of cloud computing.

Cloud computing is defined as a model for enabling service users to have ubiquitous, convenient and on-demand network access to a shared pool of configurable resources, that can be rapidly provisioned and released with minimal management effort or resource pooling provider interaction. Cloud computing enables cloud services which identified as a service that is delivered and consumed on demand at any time, through any access network, using any connected devices using cloud computing technologies. It is considered from a telecommunication perspective that users are not buying resources but cloud services that are enabled by cloud computing environments.

The cloud computing model promotes availability and is composed of six key characteristics as followings[136]:

- On-demand self-service: A cloud service user can unilaterally provision computing capabilities, such as server time, network storage and communication and collaboration services, as needed automatically without requiring human interaction with each service's cloud service provider.
- Broad network access: Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms.
- Resource pooling: The cloud service provider's computing resources are pooled to serve multiple users or organisations using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to user demand. There is a sense of location independence in that the customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify the location at a higher level of abstraction.
- Rapid elasticity: Capabilities can be rapidly and elastically provisioned, in some cases automatically, to quickly scale out, and rapidly released to quickly scale in. To the cloud service user, the capabilities available for provisioning often appear to be unlimited and can be purchased in any quantity at any time.
- Measured Service: Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service. Resource usage can be monitored, controlled, and reported. It provides transparency for both cloud service provider and cloud service users.
- Multi-tenancy: A characteristic of cloud in which resources are shared amongst multiple cloud tenants. Tenant is intended here as any Cloud Service User (CSU) workload that has unique requirements and/or a unique operating agreement with the Cloud Service Provider (CSP). There is an expectation on the part of the cloud tenant that its use of the cloud is isolated from other tenants' use in the same share resource pool.

### 5.2.2. Required Capabilities for Cloud Computing

- General Requirements for Cloud Computing[137]
- Service life-cycle management: It is required that cloud computing supports automated service provisioning, modification and termination during the service life-cycle.
- Regulatory aspects: It is required that all applicable laws and regulations be respected, including those related to privacy protection.
- Security: It is required that the cloud computing environment be appropriately secured to protect the interests of all persons and organizations involved in the cloud computing ecosystem.
- Accounting and charging: It is recommended that cloud computing supports various accounting and charging models and policies.

---

[136] References: ITU-D Question 26/2, Migration from existing networks to next generation networks for developing countries, 2014; and ITU-T Y.3500 Cloud computing – Overview and vocabulary, 2014.

[137] ITU-T Recommendation Y.3501, "Cloud Computing Framework and high-level requirements," 2013

- Efficient service deployment: It is recommended that cloud computing enables efficient use of resources for service deployment.
- Interoperability: It is recommended that cloud computing systems comply with appropriate specifications and/or standards for allowing these systems to work together.
- Portability: It is recommended that cloud computing supports the portability of software assets and data of cloud service customers (CSCs) with minimum disruption.
- Service access: Cloud computing is recommended to provide CSCs with access to cloud services from a variety of user devices. It is recommended that CSCs be provided with a consistent experience when accessing cloud services from different devices.
- Service availability, service reliability and quality assurance: It is recommended that the cloud service provider (CSP) provides end-to-end QoS assurance, high levels of reliability and continued availability of cloud services according to the SLA with the CSC.

- General Requirements for Infrastructure as a Service (IaaS)
- Configuration, deployment and maintenance of resources: IaaS CSP is recommended to configure, deploy and maintain computing, storage and networking resources to CSC.
- Use and monitoring of resources: IaaS CSP is recommended to provide the capability for CSC to use and monitor computing, storage and networking resources so that they are able to deploy and run arbitrary software.

- General Requirements for Network as a Service (NaaS)
- On-demand network configuration: It is required that the CSP provides the network capability, which can be configured on demand by the CSC.
- Secure connectivity: It is required that the NaaS CSP provides secure connectivity.
- QoS-guaranteed connectivity: The NaaS CSP is recommended to provide QoS-guaranteed connectivity according to the negotiated SLA.
- Heterogeneous networks compatibility: It is recommended that the CSP supports network connectivity through heterogeneous networks.

- General Requirements for Desktop as a Service (DaaS)
- Configurability of the virtual environment: It is recommended that a user is capable of configuring the virtual desktops' virtual environment, such as the CPU, memory, storage, network, etc.
- Fast boot-up time: The DaaS CSP is recommended to provide CSCs with appropriate boot-up time of their virtual desktops.
- QoE: The DaaS CSP is recommended to provide an acceptable user experience, including the running speed of application programs and the capability to select and run various applications, when application programs run in their CSC devices.
- Single sign-on access control: It is recommended that a CSC is capable of getting all of a DaaS functionality with the appropriate security requirements through a single sign-on mechanism.

- General Requirements for End-to-End Cloud Resource Management
- Manageability for a single cloud service: It is required that the CSP be able to collect management, telemetry and diagnostics and/or status information from components executing in various layers of cloud service implementation and report the information to the CSC.
- Manageability for multiple cloud services: It is recommended that multiple CSPs work together to offer comprehensive status awareness and management information to expand across multiple cloud data centres as composite cloud services are built from multiple services implemented by multiple cloud providers, requiring the need for multi-cloud, end-to-end management data.

- General Requirements for Cloud Infrastructure

- Resource abstraction and control: It is required for cloud infrastructure to provide resource abstraction and control capability to cloud services.
- Resource provisioning: It is required for cloud infrastructure to provide collaboratively compute, storage, and network resources to cloud services and supporting functions.

### 5.2.3. Role and Key Areas of ICT infrastructure for Cloud Computing[138]

- Cloud Computing Roles and Activities

Within the context of cloud computing, it is often necessary to differentiate requirements and issues for certain parties. These parties are entities that play roles. Roles, in turn, are sets of activities and activities themselves are implemented by components. All cloud computing related activities can be categorized into three main groups: activities that use services, activities that provide services and activities that support services.

- Cloud service customer. A party which is in a business relationship for the purpose of using cloud services. The business relationship is with a cloud service provider or a cloud service partner. Key activities for a cloud service customer include, but are not limited to, using cloud services, performing business administration, and administering use of cloud services;
- Cloud service partner. A party which is engaged in support of, or auxiliary to, activities of either the cloud service provider or the cloud service customer, or both. A cloud service partner's activities vary depending on the type of partner and their relationship with the cloud service provider and the cloud service customer. Examples of cloud service partners include cloud auditor and cloud service broker;
- Cloud service provider. A party which makes cloud services available. The cloud service provider focuses on activities necessary to provide a cloud service and activities necessary to ensure its delivery to the cloud service customer as well as cloud service maintenance.

- Cloud Capabilities Types and Cloud Service Categories

A cloud capabilities type is a classification of the functionality provided by a cloud service to the cloud service customer, based on the resources used. There are three different cloud capabilities types: application capabilities type, infrastructure capabilities type, and platform capabilities type, which are different because they follow the principle of separation of concerns. The cloud capabilities types are:

- Application capabilities type. A cloud capabilities type in which the cloud service customer can use the cloud service provider’s applications.
- Infrastructure capabilities type. A cloud capabilities type in which the cloud service customer can provision and use processing, storage or networking resources.
- Platform capabilities type. A cloud capabilities type in which the cloud service customer can deploy, manage and run customer-created or customer-acquired applications using one or more programming languages and one or more execution environments supported by the cloud service provider.

A cloud service category is a group of cloud services that possess some common set of qualities. A cloud service category can include capabilities from one or more cloud capabilities types. Representative cloud service categories are:

- Communications as a Service (CaaS). A cloud service category in which the capability provided to the cloud service customer is real time interaction and collaboration;
- Compute as a Service (CompaaS). A cloud service category in which the capabilities provided to the cloud service customer are the provision and use of processing resources needed to deploy and run software.
- Data Storage as a Service (DSaaS). A cloud service category in which the capability provided to the cloud service customer is the provision and use of data storage and related capabilities.
- Infrastructure as a Service (IaaS). A cloud service category in which the cloud capabilities type provided to the cloud service customer is an infrastructure capabilities type.
- Network as a Service (NaaS). A cloud service category in which the capability provided to the cloud service customer is transport connectivity and related network capabilities.

[138] ITU-T Recommendation Y.3501, “Cloud Computing Framework and high-level requirements,” 2013

- Platform as a Service (PaaS). A cloud service category in which the cloud capabilities type provided to the cloud service customer is a platform capabilities type.
- Software as a Service (SaaS). A cloud service category in which the cloud capabilities type provided to the cloud service customer is an application capabilities type.

- Cloud Deployment Models

Cloud deployment models represent how cloud computing can be organized based on the control and sharing of physical or virtual resources. The cloud deployment models include:

- Public cloud. Cloud deployment model where cloud services are potentially available to any cloud service customer and resources are controlled by the cloud service provider. A public cloud may be owned, managed, and operated by a business, academic, or government organization, or some combination of them. It exists on the premises of the cloud service provider.
- Private cloud. Cloud deployment model where cloud services are used exclusively by a single cloud service customer and resources are controlled by that cloud service customer. A private cloud may be owned, managed, and operated by the organization itself or a third party and may exist on premises or off premises. The cloud service customer may also authorize access to other parties for its benefit..
- Community cloud. Cloud deployment model where cloud services exclusively support and are shared by a specific collection of cloud service customers who have shared requirements and a relationship with one another, and where resources are controlled by at least one member of this collection. A community cloud may be owned, managed, and operated by one or more of the organizations in the community, a third party, or some combination of them, and it may exist on or off premises.
- Hybrid cloud. Cloud deployment model using at least two different cloud deployment models. The deployments involved remain unique entities but are bound together by appropriate technology that enables interoperability, data portability and application portability. Hybrid clouds represent situations where interactions between two different deployments may be needed but remained linked via appropriate technologies.

### 5.2.4. Architectural Overview for Cloud Computing[139]

- Functional Architecture

The functional architecture for cloud computing describes cloud computing in terms of a high level set of functional components. The functional components represent sets of functions that are required to perform the cloud computing activities. The functional architecture describes functional components in terms of a layering framework where specific types of functions are grouped into each layer and where there are interfaces between the functional components in successive layers.

- Layering Framework

The layering framework used in the cloud computing reference architecture (CCRA) has four layers of user layer, access layer, service layer and resource layer, plus a set of functions which spans across the layers. The functions which span the layers are called the multi-layer functions. The layering framework is shown diagrammatically in Figure 5-2-1.

[139] ITU-T Y.3502, "Information technology — Cloud computing - Reference architecture," Aug. 2014.

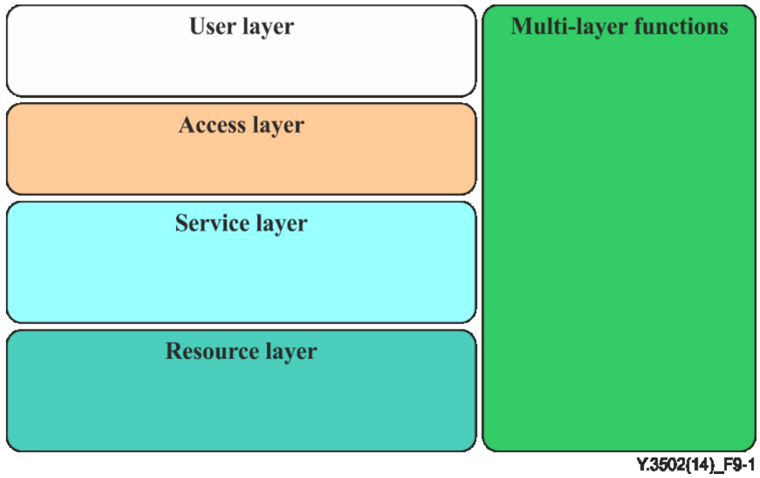


Figure 5-2-1 Cloud computing layering framework

Each of the layers in the framework is described in the following sub-clauses.

- User layer : The user layer is the user interface, through which a cloud service customer interacts with cloud service provider and with cloud services, perform customer related administrative activities, and monitors cloud services. It can also offer the output of cloud services to another resource layer instance.
- Access layer : The access layer provides a common interface for both manual and automated access to the capabilities available in the services layer. These capabilities include both the capabilities of the services and also the administration and business capabilities. The access layer is responsible for presenting cloud service capabilities over one or more access mechanisms- for example, as a set of web pages accessed via a browser, or as a set of web services which can be accessed programmatically, on secure communication. Another responsibility of the access layer is to apply appropriate security functionality to the access to cloud service capabilities.
- Service layer : The service layer contains the implementation of the services provided by a cloud service provider. The service layer contains and controls the software components that implement the services, and arranges to offer the cloud services to users via the access layer. The service implementation software in the service layer in turn relies upon the capabilities available in the resource layer to provide the services that are offered and to ensure that the requirements of any SLA relating to the services are met.
- Resource layer : The resource layer is where the resources reside. This includes equipment typically used in a data centre such as servers, networking switches and routers, storage devices, and also the corresponding non-cloud-specific software that runs on the servers and other equipment such as host operating systems, hypervisors, device drivers, generic systems management software.
- Multi-layer functions : The multi-layer functions include a series of functional components that interact with functional components of the above four other layers to provide supporting capabilities including operational support systems capabilities, business support systems capabilities, security systems capabilities, integration capabilities and development support capabilities.

- Functional Components

This clause describes the cloud architecture in terms of the common set of cloud computing functional components. A functional component is a functional element of the CCRA which is used to perform an activity or some part of an activity and which has an implementation artefact in a concrete realization of the architecture.

Figure 5-2-2 presents a high level overview of the CCRA functional components organized by means of the layering framework. For the details of each functional component, please refer to ITU-T Recommendation Y.3502.

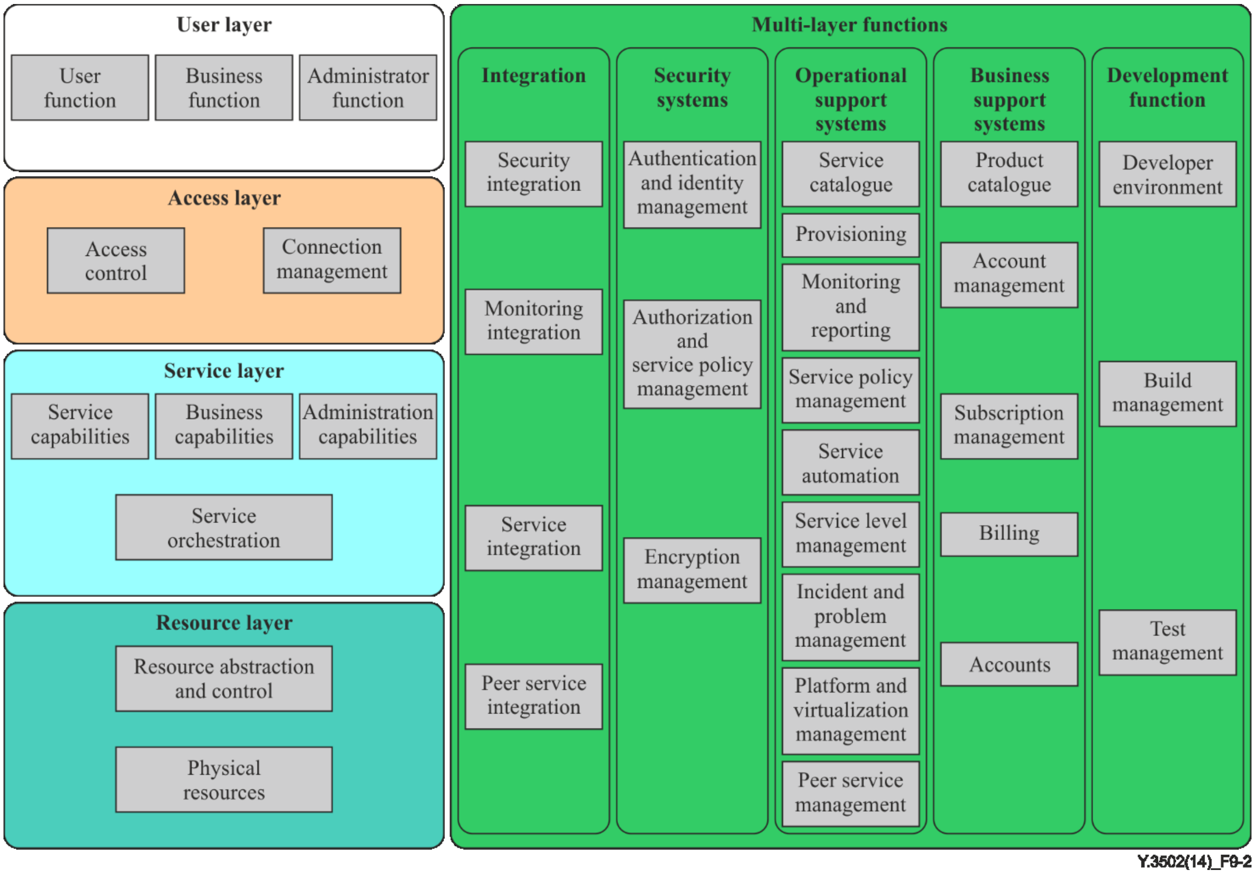



Figure 5-2-2 Functional components of the CCRA

- Generic Network Model for Cloud Infrastructure[140]

Typically, there are several types of networks involved in cloud computing services delivery and composition, such as the intra-datacentre network and inter-datacentre network, as well as the access and core transport network, etc.

To illustrate the cloud computing network concepts described, a generic network model, which supports cloud computing infrastructure, is shown in Figure 5-2-3 The generic network model is described as follows:

- Intra-datacentre network: The network connecting local cloud infrastructures, such as the datacentre local area network used to connect servers, storage arrays and L4-L7 devices.
- Access and core transport network: The network used by CSCs to access and consume cloud services deployed by the CSP.
- Inter-datacentre network: The network interconnecting remote cloud infrastructures. These infrastructures may be owned by the same or different CSPs; an inter-datacentre network primarily supports the following two scenarios:
  - Workload migration, which means moving workloads from an enterprise datacentre to a CSP datacentre, or moving workloads from CSP to CSP.
  - Server clustering which allows transactions and storage replication for the business continuity.

A centralized resource abstractor and controller ensures the overall management of the cloud environment with:

- Network management systems that are dedicated to network service providers. The processes supported by network management systems include management and maintenance of the network inventory, and the configuration of network components, as well as fault management.

[140] ITU-T Recommendation Y.3510, "Cloud computing infrastructure requirements," May 2013.

• Cloud management systems are dedicated to CSPs. Cloud management systems support processes for maintenance, monitoring and configuration of cloud infrastructure resources.

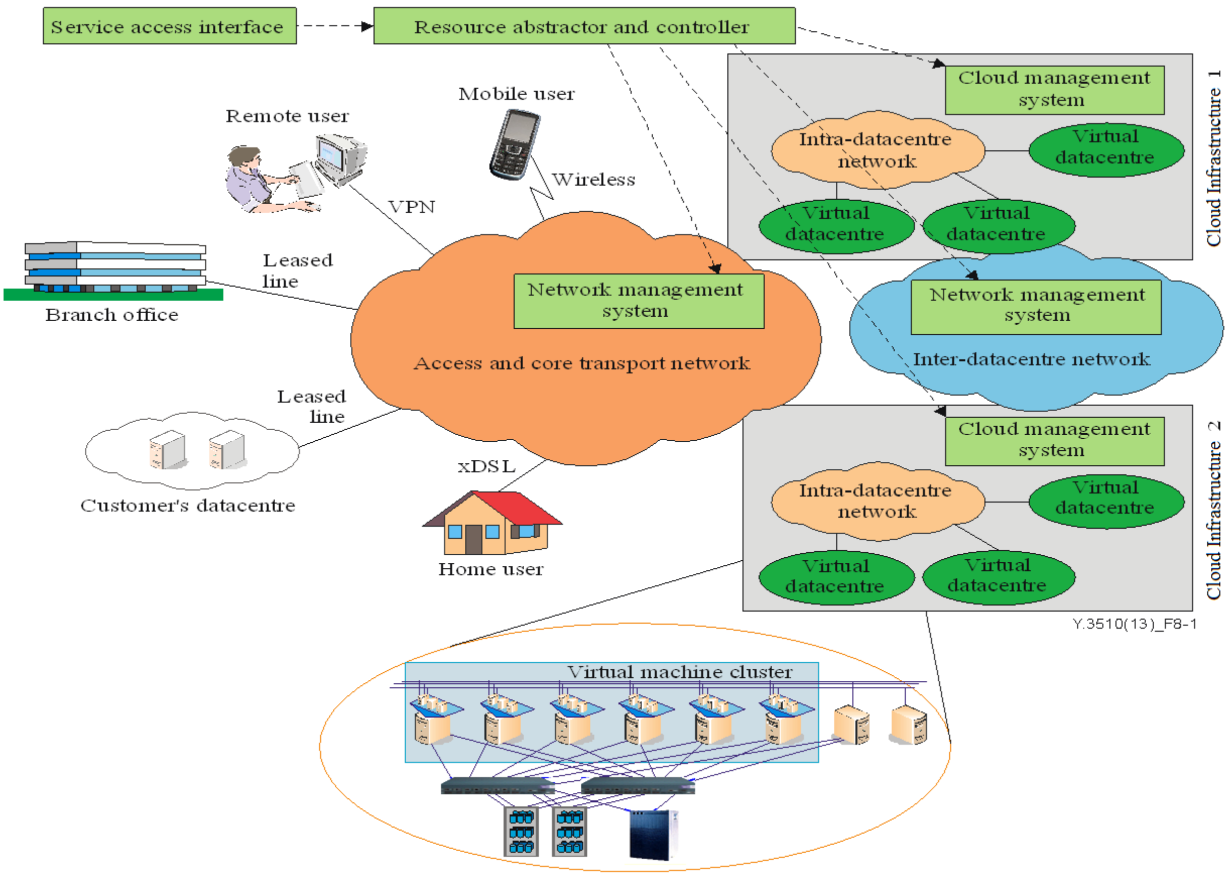



Figure 5-2-3 Generic network model for cloud infrastructure

### 5.2.5. Standardization for Cloud Computing

Cloud computing is an industry expected to grow at an annual growth rate of roughly 30 per cent, consequently more than quadrupling in size between 2010 and 2015 to become an industry worth approximately $120 billion. However, concerns with the portability – freedom to transfer data between the clouds of different providers - and the interoperability of cloud solutions has led to calls for standardization to fuel further industry growth[141].

There are many activities for standardization on cloud architecture and related services. The followings are the latest update for cloud standardization:

- ITU-T
- ITU-T Focus Group on Cloud Computing (FG-Cloud) had developed key deliverables on use cases, requirements & architecture, cloud security, infrastructure & network enable cloud, cloud services & resource management, platform and middleware with the telecommunication aspects. In addition, this group collaborated with worldwide cloud computing communities including other SDOs and consortia.
- ITU-T's SG 13 has created a new Working Party (WP) on cloud computing, tasked with progressing the Technical Reports that were the output of a previous FG-Cloud towards formalization as ITU-T Recommendations.

[141] ITU-T TechWatch Report, "Distributed Computing: Utilities, Grids and Clouds"

- There are newly established 3 Questions:
  - Cloud computing ecosystem, inter-cloud and general requirements
  - Cloud functional architecture, infrastructure and networking
  - Cloud computing resource management and virtualization
- National Institute of Standards and Technology (NIST)
- NIST provides technical guidance for secure applications in government and industry. NIST promotes relevant technical standards, and its definition of cloud computing is also considered an industry standard.
- Distributed Management Task Force (DMTF)
- DMTF is an industry organization that develops, maintains and promotes standards for systems management in enterprise IT environments.
- Storage Networking Industry Association (SNIA)
- SNIA is a non-profit trade association founded in 1997 with headquarters in San Francisco. SNIA promotes standards, technologies and educational services for the storage industry.
- Open Cloud Consortium (OCC)
- OCC is a group of American universities that seeks to improve cloud performance, promotes open frameworks for interoperation between clouds, and develops reference implementations, benchmarks and standards for cloud computing. OCC also manages the open cloud test bed and open science data cloud.
- Open Grid Forum (OGF)
- OGF is a community of users, developers, and vendors leading efforts to standardize grid computing. The OGF community consists of thousands of individuals from over 400 industry and research organizations in more than 50 countries.
- Cloud Security Alliance (CSA)
- The CSA is a not-for-profit organization with a mission to promote the use of best practices for providing security assurance within Cloud Computing, and to provide education on the uses of Cloud Computing to help secure all other forms of computing.
- The Telecom Working Group (TWG) within the CSA has been designated to provide direct influence on how to deliver secure cloud solutions and foster cloud awareness within all aspects of Telecommunications.

Additionally, the following groups are also related to cloud computing standardization:

- ISO/IEC JTC1 SC38 Study Group on Cloud Computing (SGCC)
- Cloud Computing Interoperability Forum (CCIF)

- **ITU related Documents**[142]

| No | Group | Document title | Scope of document | Status |
|---|---|---|---|---|
| **1** | JRG-CCM* | **M.occm** Overview of Cloud Computing Management | This Recommendation is to identify the difference between cloud computing management and traditional telecom management, including the management activities and management objects, and the new management requirements from the point view of telecom operator, and to provide an overview and framework for the cloud computing management. | Under study |
| **2** | JRG-CCM* | **M.rcsm** Requirements for cloud service management | This recommendation identifies the relationship between cloud service management and cloud resource management, defines the general management requirements and management function requirements that support the cloud service fulfilment, operation, and provides function framework for cloud services management. | Under study |
| **3** | JRG-CCM* | **M.mivrcc** Requirements and analysis for management interface of virtual resource in cloud computing | This draft Recommendation specifies the requirements and analysis for the management interface between the cloud operational support system (COSS) and the virtualized resource management (VRM) agent. This draft Recommendation follows the interface specification methodology described in [ITU-T M.3020]. | Under study |
| **4** | ITU-T SG11 Q.14 | **Q.FW-Cloud-iop** The framework and overview of Cloud Computing interoperability testing | This Recommendation describes the framework and overview of Cloud Computing interoperability testing. The framework Recommendation includes general scenarios and kinds of testing and measurement technologies for interoperability testing of cloud computing. | Under study |
| **5** | ITU-T SG11 Q.14 | **Q.Supp-CCI** Supplement Q-series: Cloud computing interoperability activities | This supplement describes the summary information of cloud computing interoperability activities of existing standards development organizations and the groups, forums, open source developing the specifications that have potential utilized to cloud computing interoperability testing tools. | Under study |
| **6** | ITU-T SG13 | **Y.3501** Cloud computing framework and high-level requirements | This Recommendation provides a cloud computing framework by identifying the high-level requirements for cloud computing. It addresses the general requirements and use cases for cloud computing, infrastructure as a service (IaaS), network as a service (NaaS), and desktop as a service (DaaS) cloud services. | Published (5/2013) |
| **7** | ITU-T SG13 | **Y.3503** Requirements for Desktop as a Service | This Recommendation provides use cases, general requirements and functional requirements for Desktop as a Service (DaaS). | Published (5/2014) |
| **8** | ITU-T SG13 | **Y.3510** | This Recommendation identifies requirements for cloud infrastructure capabilities to support cloud services. The scope of this Recommendation includes overview of cloud infrastructure, requirements for compute resources, requirements for network resources, etc. | Published (5/2013) |

142 The information in this list is subject to change according to the group`s developments. For latest information please see http://itu.int/go/B21L.

| | | | | |
|---|---|---|---|---|
| | | Cloud computing infrastructure requirements | | |
| **9** | ITU-T SG13 | **Y.3511** Framework of inter-cloud computing | This Recommendation describes the framework for interactions between multiple cloud service providers (CSPs) that is referred to as inter-cloud computing. Based on use cases involving several CSPs and consideration on different types of service offerings, this Recommendation describes the possible relationships among multiple CSPs, interactions between CSPs, and relevant functional requirements. | Published (3/2014) |
| **10** | ITU-T SG13 | **Y.3520** Cloud computing framework for end-to-end resource management | This Recommendation provides a framework for end-to-end resource management in cloud computing. It includes:<br>• general concepts of resource management for end-to-end cloud computing resource management.<br>• a vision for adoption of resource management for cloud computing.<br>• multi-cloud, end-to-end management of cloud computing resources and services. | Published (6/2013) |
| **11** | ITU-T SG13 | **Y.3500** Cloud computing - Overview and Vocabulary | This Recommendation provides an overview of cloud computing along with a set of terms and definitions. It is a terminology foundation for cloud computing standards. This Recommendation is applicable to all types of organizations. | Consented (7/2014) |
| **12** | ITU-T SG13 | **Y.3502** Cloud computing - reference architecture | This Recommendation specifies the cloud computing reference architecture (CCRA). The reference architecture includes the cloud computing roles, cloud computing activities as well as the cloud computing functional components and their relationships. | Consented (7/2014) |
| **13** | JRG-CCM | **Y.e2ecslm-Req** End-to-end cloud service lifecycle management requirements | This Recommendation specifies the functional requirement of the lifecycle for service management aspects of Cloud services. The Cloud service lifecycle management involves charging events management, policy management, management of role related information, service/application provisioning, resource management, context management, and content management [ITU-T Y.2240]. | Under study |
| **14** | ITU-T SG17 | **X.1601** Security framework for cloud computing | This Recommendation analyses security threats and challenges in the cloud computing environment, and describes security capabilities that could mitigate these threats and address security challenges. A framework methodology is provided for determining which of these security capabilities will require specification for mitigating security threats and addressing security challenges for cloud computing. | Published (1/2014) |
| **15** | ITU-T SG17 Q.8 | **X.goscc** Guidelines of operational security for cloud computing | The Recommendation clarifies security responsibilities between CSPs and CSUs, and analyses the requirements and categories of security metrics for cloud computing. It defines sets of security policies and security activities for daily operation and maintenance for cloud computing services and infrastructure from the perspective of CSPs, to fulfill the requirements of operational security for cloud computing. | Under study |
| **16** | ITU-T SG17 Q.10 | **X.idmcc** Requirements of IdM in cloud computing | This Recommendation provides use-case and requirements analysis giving consideration to the existing industry efforts. This Recommendation concentrates on the requirements for providing IdM as a Service | Under study |

| | | | | |
|---|---|---|---|---|
| | | | (IdMaaS) in cloud computing. The use of non-cloud IdM in cloud computing, while common in industry, is out of scope for this Recommendation. | |

*JRG-CCM – Joint Rapporteur Group on Cloud Computing Management. For more information see http://itu.int/go/PPLR.

## 5.3 Smart Grid

### 5.3.1. Overview[143]

- Concept of Smart Grid

Among Smart Grid research and development activities, there is not currently a globally agreed the definition for "The Smart Grid". However, it has been already recognized that the Smart Grid is a new electricity network, which highly integrates the advanced sensing and measurement technologies, information and communication technologies (ICTs), analytical and decision-making technologies, automatic control technologies with energy and power technologies and infrastructure of electricity grids. Some important aspects of what 'smart' are listed below:

- Observability: It enables the status of electricity grid to be observed accurately and timely by using advanced sensing and measuring technologies;
- Controllability: It enables the effective control of the power system by observing the status of the electricity grid;
- Timely analysis and decision-making: It enables the improvement of intelligent decision-making process;
- Self-adapting and self-healing: It prevents power disturbance and breakdown via self-diagnosis and fault location.
- Renewable energy integration: It enables to integrate the renewable energy such as solar and wind, as well as the electricity from micro-grid and supports efficient and safe energy delivery services for electric vehicle, smart home and others.

- Goals and Objectives of Smart Grid

Efficient and reliable transmission and distribution of electricity is a fundamental requirement for providing societies and economies with essential energy resources. The utilities in the industrialized countries are today in a period of change and agitation. On one hand, large parts of the power grid infrastructure are reaching their designed end of life time, since a large portion of the equipment was installed in the 1960s. On the other hand, there is a strong political and regulatory push for more competition and lower energy prices, more energy efficiency and an increased use of renewable energy like solar, wind, biomasses and water.

In industrialized countries, the load demand has decreased or remained constant in the previous decade, whereas developing countries have shown a rapidly increasing load demand. Aging equipment, dispersed generation as well as load increase might lead to highly utilized equipment during peak load conditions. If the upgrade of the power grid should be reduced to a minimum, new ways of operating power systems need to be found and established.

In many countries, regulators and liberalization are forcing utilities to reduce costs for the transmission and distribution of electrical energy. Therefore, new methods (mainly based on the efforts of modern information and communication techniques) to operate power systems are required to guarantee a sustainable, secure and competitive energy supply.

The general goals of Smart Grid are to ensure a transparent, sustainable and environmental-friendly system operation that is cost and energy efficient, secure and safe. Objectives of developing the Smart Grid are quite different from country to country for their various demands and start points. However, the common objectives of a Smart Grid are clear and listed below:

- Robustness: The Smart Grid shall improve resilience to disruption to provide continuous and stable electricity flows, avoiding wide-area breakout accidents. It shall guarantee the normal and secure run of the electricity grid even under the instance of emergency issues, such as natural disasters, extreme weather and man-made breakage, and provides self-healing abilities;
- Secured operation: The Smart Grid shall enhance communication networks and information security of the electricity grid;
- Compatibility: The Smart Grid shall support the integration of renewable electricity such as solar and wind, has the capacity of distributed generation access and micro-grids, improve demand response functions, implement the effective two-way communication with consumers and satisfy various electricity demands of consumers;

---

[143] ITU-T FG-Smart Deliverables, ITU-T Y.MEG (Framework of micro energy grid)

- Economical energy usage: The Smart Grid shall have the capacity of more effective electricity markets and electricity trades, implement optimized configuration of resources, increase efficiency of the electricity grid, and reduce electricity grid wastage;
- Integrated system: The Smart Grid shall highly integrate and share information and data of an electricity grid, utilize the uniform platform and model to provide standardized and refined management;
- Optimization: The Smart Grid shall optimize assets, reduce costs and operate efficiently;
- Green energy: The Smart Grid shall solve problems of energy security, energy saving, carbon dioxide emission and etc.

The utilities of the Smart Grid shall address the following challenges:

- High power system loading;
- Increasing distance between generation and load;
- Fluctuating renewables;
- New loads (hybrid/electric vehicles);
- Increased use of distributed energy resources;
- Cost pressure;
- Utility unbundling;
- Increased energy trading;
- Transparent consumption & pricing for the consumer;
- Significant regulatory push.

The key market drivers behind Smart Grid solutions are:

- Need for more efficient use of energy;
- Increased usage of renewable energy resources;
- Sustainability;
- Competitive energy prices;
- Security of supply;
- Ageing infrastructure and workforce.

The priority of local drivers and challenges might differ from place to place.

- Micro Energy Grid

The concept of micro energy grid (MEG) is proposed so as to enhance the local reliability and flexibility of electric power systems, which may consist of multiple distributed energy resources (DERs), customers, energy storage units. The MEG can be further defined as a small electric power system being able to operate physically islanded or interconnected with the utility grids.

NOTE - Due to increasing shortage of the fossil fuel and the impelling pressures from environmental protection, new generation sources of high efficiency such as fuel cell and microgas turbine, as well as renewable energy sources (RESs) such as wind and solar power, are becoming the most important DERs.

From the concept of MEG, MEG has the following benefits: Power is generated where it is needed, Ease of renewable energy integration, Local control and ownership, Reduction in transmission losses and carbon footprint, Stand-alone grid and operation in isolation mode in case of blackout, finally Easy to finance and faster to build.

The prosumer in MEG is an economically motivated entity that consumes and produces electricity, operates or owns a power system that contains sources, loads, and possibly energy storage, and who optimizes the economic decisions regarding its energy utilization. The prosumer can be an owner of DER and storage as well as a consumer as follows:

- DER Owner (Person/Organization): The DER Owner (or DG Owner) operates a Distributed Energy Resource (DER) (or Distributed Generation (DG)) which is connected to the micro energy grid.
- Consumer (Person/Organization): A consumer of electricity which is a private, business building, large industrial / manufacturing industry or transportation system. The consumer acts as a customer. The consumer may operate Smart Appliances (an electrical load with some intelligence to control it) which are flexible in demand.
- Storage Owner (Person/Organization): Provider of storage capacity for storing and delivering energy.

Therefore, the prosumer consumes energy, produces energy, stores energy and participates in a market externally. In addition, it operates a power system and economically optimizes its energy use internally.

MEG must meet several requirements to enable seamless operation. To support MEG, some important top-level features should be considered in standardization:

- Autonomy: MEG includes generation, storage, and loads, and can operate autonomously in grid-connected and islanded mode.
- Stability: Independent local control of generators, batteries, and loads of MEG are based on frequency droops and voltage levels at the terminal of each device. This means that MEG can operate in a stable manner during nominal operating conditions and during transient events, no matter whether the larger grid is up or down.
- Compatibility: MEG is completely compatible with the existing utility grid. MEG may be considered as functional units that support the growth of the existing system in an economical and environmentally friendly way.
- Flexibility: The expansion and growth rate of MEG does not need to follow any precise forecasts. The lead times of corresponding components (fossil-fueled and renewable generators, storage systems, and others) are short, and MEG can grow incrementally. MEG is also technology-neutral and able to cope with a diverse mixture of renewable and fossil-fueled generators.
- Scalability: MEG can simply grow through the additional installation of generators, storage, and loads. Such an extension usually requires an incremental new planning of the MEG and can be performed in a parallel and modular manner in order to scale up to higher power production and consumption levels.
- Efficiency: Centralized as well as distributed MEG supervisory controller structures can optimize the utilization of generators, manage charging and discharging energy storage units, and manage consumption. In this way energy management goals can be profoundly optimized, for example in economic as well as environmental respects.
- Economics: According to market research studies, economics of heat recovery and its application by CHP systems is very important to the evaluation of MEG. In addition, the utilization of renewable energy resources will help reduce fuel costs and CO2 emissions.
- Peer-to-peer model: MEG can support a true peer-to-peer model for operation, control, and energy trade. In addition, interactive energy transactions with the centralized utility grid are also possible with this model.

- Conceptual model and reference diagram for Smart Grid

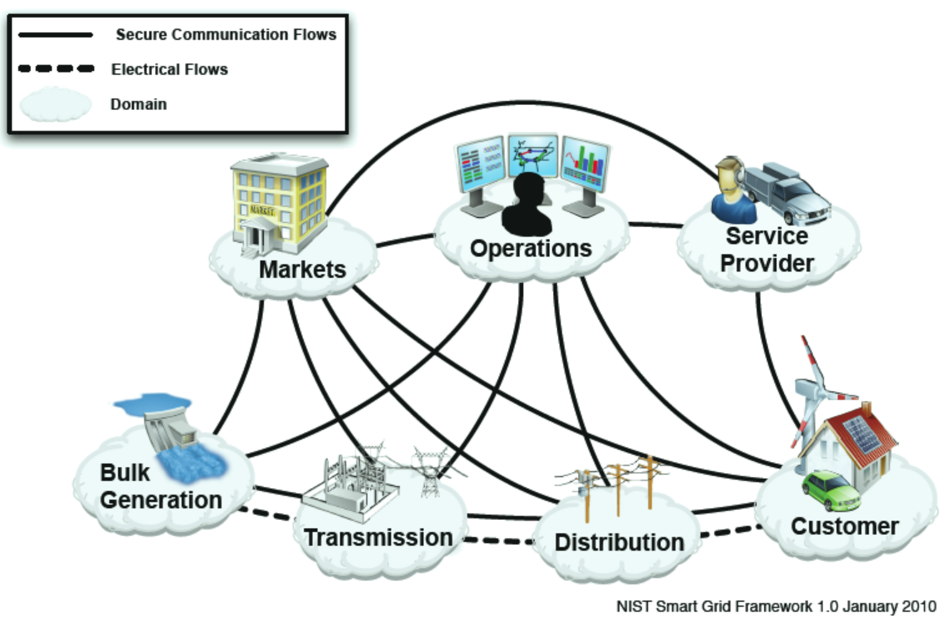



Figure 5-3-1. A conceptual model of Smart Grid

Figure 5-3-1, extracted from the NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 2.0 document, shows a conceptual model of Smart Grid, consisting of seven major functional area call domains and the information flows between these domains, as well as the flow of electricity from power sources through transmission and distribution system to the customers. Table 5-3-1 gives a brief definition of these domains[144,145].

An important new capability for Smart Grid not explicitly shown in this model is the distributed power generation that may occur in the Customer, Distribution, and Transmission domains. If the generation facility exists in the Customer domain, a new paths for electrical and communication flows need to be shown; similarly for generation capabilities in the Transmission and Distribution domains.

Table 5-3-1. Domains and Actors in the Smart Grid conceptual model

| Domain | Actors in the Domain |
|---|---|
| Customers | The end users of electricity. May also store, and manage the use of energy. Traditionally, three customer types are discussed, each with its own domain: residential, commercial, and industrial. |
| Markets | The operators and participants in electricity markets. |
| Service Providers | The organizations providing services to electrical customers and utilities. |
| Operations | The managers of the movement of electricity. |
| Bulk Generation | The generators of electricity in bulk quantities. May also store energy for later distribution. |
| Transmission | The carriers of bulk electricity over long distances. May also store and generate electricity. |
| Distribution | The distributors of electricity to and from customers. May also store and generate electricity. |

Figure 5-3-2 is a conceptual reference diagram for Smart Grid Information Network from the NIST document, showing the interconnections of networks between various domains. Some of networking clouds have been moved outside of individual domains to emphasize the communication functions between the domains. The major component is a backbone network, or WAN that distributes messages between domains. There is another network cloud that aggregates/de-aggregates local traffics in some domains to/from the WAN, similar to Access Networks such as optical, cable or DSL. In the Smart Grid environment, the access network is needed for connection to smart meters and customer premises, and is called Neighbourhood Network in this context as they form the networking infrastructure within each neighbourhood. The clouds labelled "Internet/e-Business" refers to the existing Internet accessible to the public, and is shown separately to indicate logical separation due to security considerations.

Within each domain, there are network infrastructures to serve the need of the domain. Of special interest to Smart Grid is the Home Area Network (HAN) in the Customer domain for Smart Grid applications, connecting various devices, such as home appliances, sensors, electric vehicle chargers, and local generators. The HAN may or may not be the same network as the existing LAN in the homes for access to Internet, depending on the security considerations of the Smart Grid.

---

[144] National Institute of Standards and Technology, "NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 1.0," January 2010

[145] Smart Grid Interoperability Panel, Smart Grid Architecture Committee, "Smart Grid Conceptual Model," April 2010

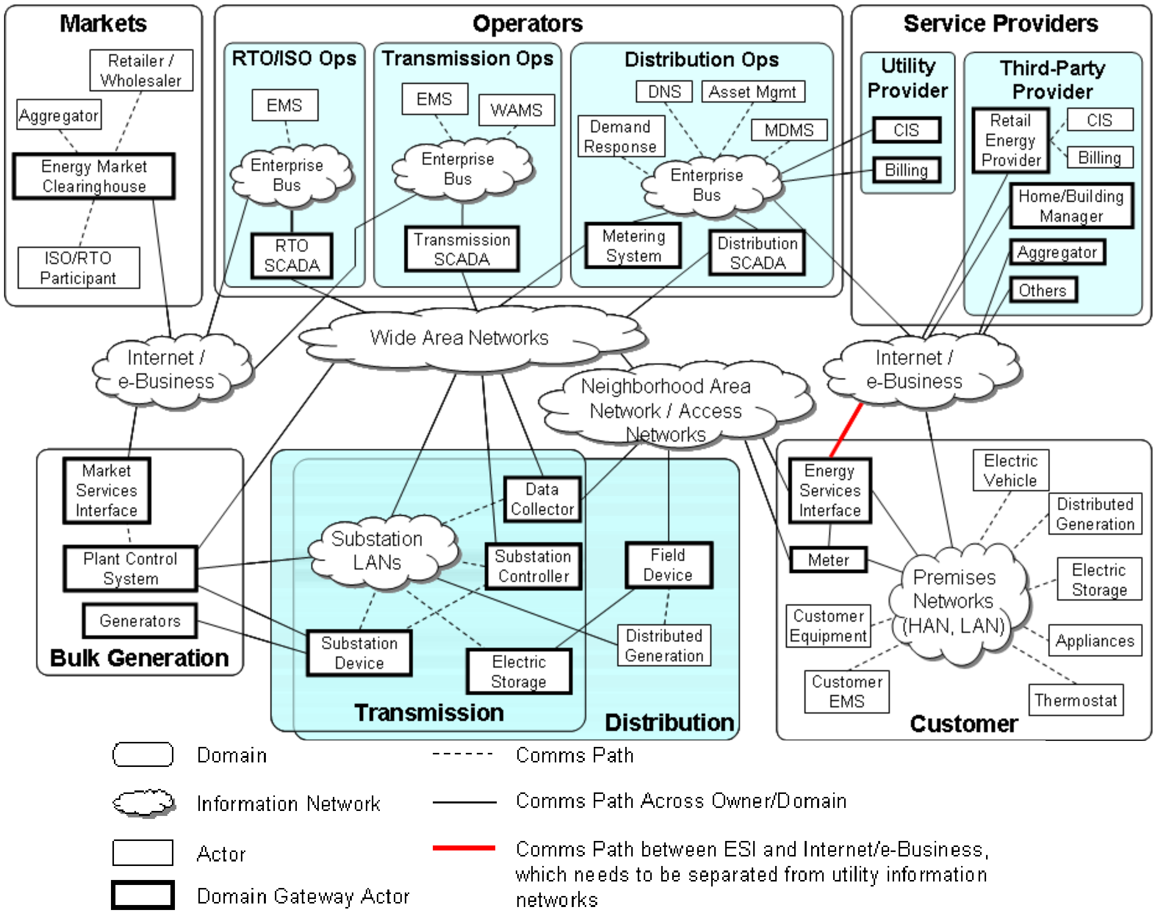


Figure 5-3-2. Conceptual Reference Diagram for Smart Grid

- Fundamental characteristics of Smart Grid

Smart Grid has the following fundamental characteristics:

- Use of information, computing, networking technologies to support the envisioned Smart Grid services: energy distribution management, energy trading, grid monitoring and management, distributed renewable energy integration, electric vehicles charging, distributed energy storage, and smart metering infrastructure;
- The Smart Grid services involve many parties across many domains, in particular active participation of customers is essential;
- Smart Grid requires new capabilities in each functional plane to achieve its goal of energy efficiency, reliability, and automation, such as new algorithms in the Services/Applications plane, security and QoS-awared two-way communications in the Communication plane, two-way transmission capability, storage techniques, and new intelligent sensors/controllers in the Energy plane;
- In order to support these services, the ICT systems must
  - provide wide range of applications such as home, building, and factory energy management systems, on demand meter readings, demand and response systems, electrical grid status monitoring, fault detection, isolation, and recovery;
  - manage wide variety of devices such as intelligent sensors, smart meters, smart appliances, and electric vehicles;
- The network infrastructure must provide reliable two-way communication and support various class of QoS, such as real-time and non-real-time, and different bandwidths and latency, loss, and security requirements;
- To ensure the interoperability of applications and devices, interoperable standards are required for communications, information representations and exchanges;
- Security of services, applications, devices in all domains, including the networks are of paramount importance to the stability and integrity of the Smart Grid.

### 5.3.2. Required Capabilities for Smart Grid[146]

- Services/Applications Plane

The following describes essential capabilities for the services/applications plane:

- Distributed network operation and management, including real-time communicate, monitor and control the status of devices in energy generation, transmission, and distribution;
- Management energy asset management and meter data management (i.e., energy usage, energy generation, meter logs, and meter test results);
- Fault management enhance the speed at which faults can be located, identified, and sectionalized and service can be restored;
- Customer and account management, and installation management;
- Billing/ account management, home management, building management, and others;
- Distributed energy resource aggregation, wholesaler & retailer marketing; and
- Dynamic pricing, trading, and market management.

- Communication Plane

The communication (control & connectivity) plane includes communication network domain. The following describes essential capabilities for the communication plane. The protocols and functional requirements are described in the Requirement deliverable following this Overview deliverable.

- Capability of IP base transport
  - Support capability of IP base transport, such as IPv4 and/or IPv6.
- OAM function
  - Failure detection and alarm transfer;
  - Hierarchical operations for failure detection and alarm transfer;
  - Communication path trace;
  - Performance measurement.
- Protection and restoration
  - Support of one or more types according to target performance, e.g., service outage period, localization, useless traffic load;
  - Co-operations among types without contradiction.
- Traffic engineering and QoS control
  - SLA guidelines, traffic provisioning and traffic control.
- Connectivity and routing
  - Reach ability based IP capability;
  - Specific signaling protocol, e.g., Session Initiation Protocol (SIP);
  - Static routing.
- Access control
  - Various types of access interfaces: wired access (e.g., Optical, xDSL, Coaxial, Power Line Communication (PLC)), wireless access (e.g., Cellular, WiFi, ZigBee, Bluetooth, other sensor)
  - Poling, demand assignment, no prevention access, etc.
- Network security147
  - Authentication;
  - Encryption.
- Network management
  - Monitor/surveillance of networks to manage failure, topology, performance, etc;
  - Monitor/surveillance of communication component to manage component type, failure, etc;
  - Provisioning of operation parameter;
  - Remote testing;
  - Compression of information;

---

146 ITU-T FG-Smart Deliverables, ITU-T Y.MEG (Framework of micro energy grid)

147 Communication should be protected from attack and virus. These protection functions should be implemented at ingress points of network. Moreover, recently, CYBEX (Cybersecurity information exchange framework) has been discussed for NGN and Cloud computing as new enhanced network security. This will be applied to Smart Grid communication network.

  - Northbound interface for communication from/to the higher network management entity.
- End networked device management
  - Management of end devices in energy plane, such as electric vehicle, distributed generation, electric storage or appliances.
- Data management
  - Data aggregation, suppression and unification of interface to reduce traffic load of communication network.

- Energy Plane

Energy plane includes grid domain, customer domain and smart metering. This plane consists of energy generation, storage, and consumption devices with communication interfaces. Information through these interfaces is transferred on communication network. The following describes essential capabilities for each domain of the energy plane.

The following describes essential capabilities for bulk generation, distribution and transmission in grid domain (bulk generation, distribution and transmission):

- Monitor and control energy generation, transmission, and distribution;
- Store and integrate renewable energy.

The following describes essential capabilities for Advance d Metering Infrastructure (AMI) in smart metering:

- Support meter reading and network interface for remote meter data reading from service provider domain;
- Provide the home area networking with direct access to consumer-specific usage data, i.e., instantaneous usage, interval usage, volts, amps, VAR, power factor, and others.

The following describes essential capabilities for customers in customer domain:

- Home/ building energy automation;
- Energy management (including control & logging);
- Renewable energy management (store, manage, and integration);
- Support electric vehicles charging;
- Manage home appliance;
- Home area networking and management;
- Supports load control: a load control device (e.g. smart appliance, pool pump controller, Energy Management System (EMS), etc.) has the capability to reduce the peak power consumption of the equipment under its control.

- Common required capabilities in all of planes

In all of planes, the following capabilities for security are required.

- Confidentiality: The Smart Grid should preserve authorized restrictions on information access and disclosure during communications, including means for protecting personal privacy and proprietary information. A loss of confidentiality is the unauthorized disclosure of information;
- Data & User privacy: Data must be treated as personal and aggregation and removal of personal details may be required. The Smart Grid should preserve authorized restrictions on information access and disclosure during use & storage, including means for protecting personal privacy and proprietary information. A loss of Data & User privacy is the unauthorized disclosure of information during use & storage;
- Integrity: Smart Grid should prevent against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. A loss of integrity is the unauthorized modification or destruction of information;
- Availability: Smart Grid should ensure timely and reliable access to and use of information. A loss of availability is the disruption of access to or use of information or an information system;

The following issues need to be considered when considering the above security features:

- Extensive data gathering and two-ways information flows may broader the potential for compromises of data confidentiality and breaches of customer privacy, and compromises of personal data and intrusion of customer privacy;
- The complexity of the grid could introduce vulnerabilities and increase exposure to potential attackers and unintentional errors;

- Increased number of entry points and paths are available for potential adversaries to exploit.

- Requirements and capabilities for micro energy grid

Micro Energy Grid has the following high-level requirements:

- It is required to provide open interfaces for easily supporting new applications and services to various stakeholders (e.g., service provider, consumer, etc.).
- It is required to support decentralized control for distributed generation and consumption.
- It is required to measure demands, generations and status of each MEG asset at various locations across the MEG network.
- It is required to automatically configure and install new devices or systems for MEG.
- It is required for a communication network to carry data across the various resources.
- It is required to interact with operators or any client or server to demonstrate and archive the MEG real-time data and receive the required commands and information.
- It is required to ensure interoperability between different information/communication models in the MEG domain.
- It is required to self-organize systems and dynamically coordinate controllers for the recovery in case of problems (e.g., black out).
- It is required to support highly secure and safe communications for the MEG services.
- It is required to minimize the total operation costs subject to different constraints and apply them automatically to the MEG assets.

Micro Energy Grid networks have the following high-level requirements:

- Fault tolerance for reliability
- Seamless transfer between wired and wireless networks
- Self-healing via topological reconfigurations
- Communication security
- Multi-point to multi-point data transfer in forming mesh network

### 5.3.3. Role and Key Areas of ICT infrastructure for Smart Grid[148]

- Concepts and roles for Smart Grid in the ICT perspective

Information and communication system is the fundamental of achieving intelligent management and control in the grid. It builds up two-way information channel between grid and consumer to achieve interaction, such as demand response, real-time price, and home energy management. The automation level of grid is improved by implementing ICT for auto-collecting and analyzing grid information.

By establishing unified and open communication infrastructure and standard system, the 'plug and play' environment could be formed to facilitate the networked communication between elements in grid and the interoperability between sensors, intelligent electronic devices and application systems. Therefore, the robustness and ability of self-healing of grid are strengthened.

Smart Grid is a power system in which the power generation, delivery and consuming are information-driven. ICT plays the core role of information collection, transfer, processing and management in Smart Grid. By means of ICT, two-way communication channel between energy relevant elements and corresponding operation units can be interconnected in Smart Grid. Therefore, it is able to reach every energy relevant element to implement information collection, such as generation capability, consumer demand, each part of power delivery, for sensing comprehensive grid situation. In this case, the reliable, safe and efficient match between power supply and demand can be achieved by intelligent information processing, decision and control implement.

To summarize, to build a future-oriented, smart, secure, efficient power system, ICT plays a critical role.

- Key areas for standardization

As shown in Figure 5-3-3, key areas for Smart Grid standards include:

- Technologies for automated energy management and decentralized power generation in customer premises, including home, building, and factories;

[148] ITU-T FG-Smart Deliverables

- Intelligent grid management at the power transport and distribution level;
- Smart meters and AMI;
- Information and communication infrastructure to provide energy intelligence, control and security;
- Applications and services for the coordination the energy system on the business level;
- Security control and management with the different level of requirements for Smart Grid.

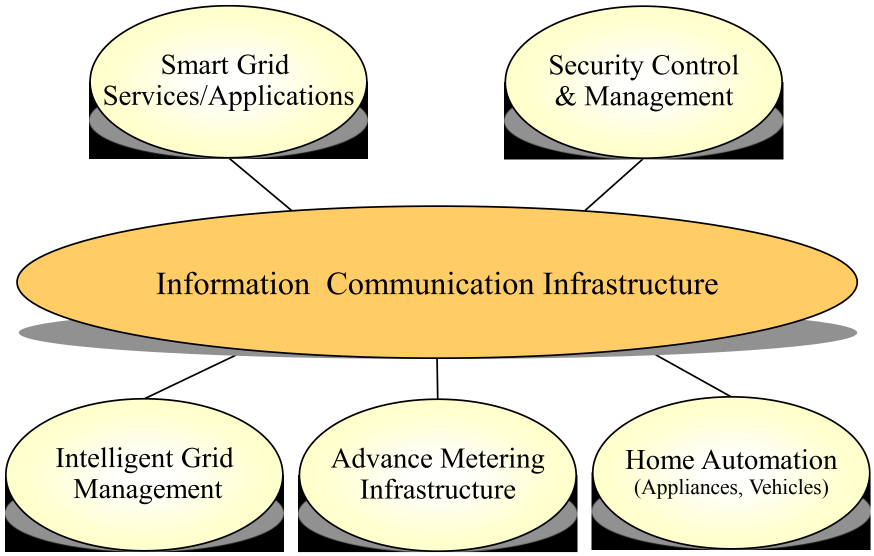



Figure 5-3-3. Key areas for standardization in the ICT perspective

- Key applications and platform in Smart Grid

In this section, we present the key applications in Smart Grid and the platform to support those applications from ICT perspective. As shown in Figure 5-3-4, we list the reprehensive applications.

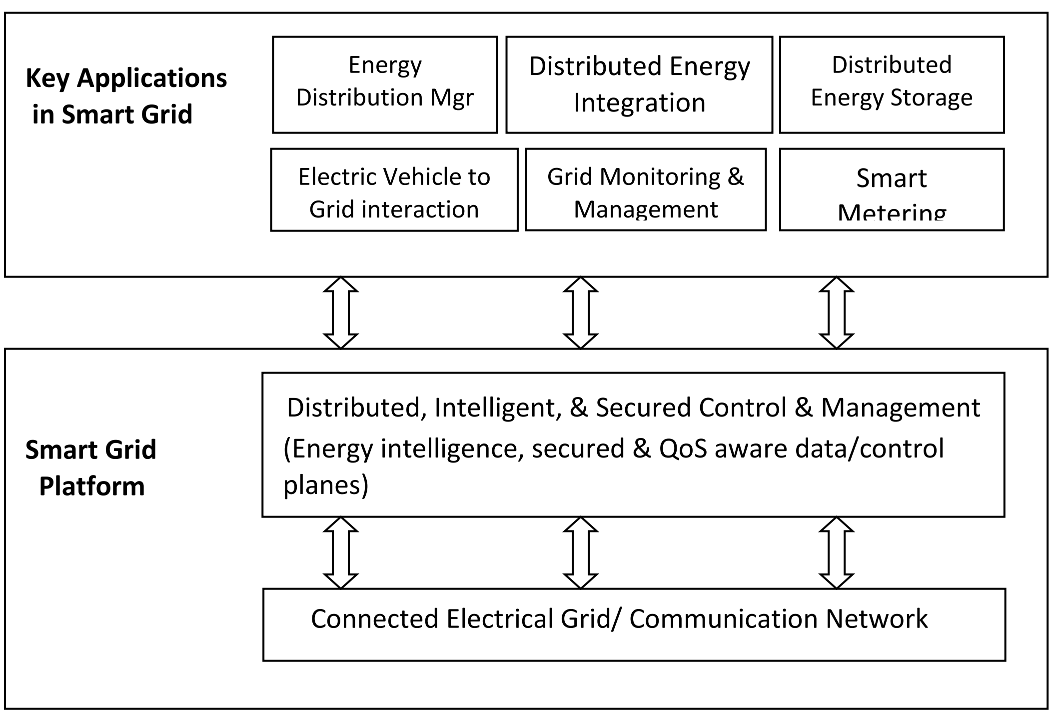



Figure 5-3-4. Key Applications and Platform in Smart Grid

- Energy distribution management: The goal of this application is to make the energy distribution system more intelligent, reliable, and self-repairing, self-optimizing. This application enables the monitoring and display of grid system components and performance across interconnections and over large geographic areas in near real-time. It includes the deployment of ubiquitous networked sensors, the software system to understand and ultimately optimize the management of grid-network components, behaviour, and performance, as well as to anticipate, prevent, or respond to the problems before disruptions can arise.
- Distributed renewable energy integration: The goal of this application is to integrate distributed renewable-energy generation facilities, including the use of renewable resources (i.e., wind, solar, thermal power, and others, as part of total energy sources. This application includes the projection of expected demand, the prediction of alternative generation capacities, and the integration of distributed generation into the distribution grid. Energy generation in a customer and micro-grid environment will require the bidirectional metering, and bidirectional energy distribution networks, which will be supported by Smart Grid.
- Distributed energy storage: In order to evenly distribute the demand and consequently lowering the need for peak generation facilities, this application enables new storage capabilities of energy in a distributed fashion, and mechanisms for feeding energy back into the energy distribution system.
- Electric vehicles to grid interaction: This application refers, primarily, to enabling large-scale integration of plug-in electric vehicles (PEVs) into the transportation system. The major challenge is the supports of PEV charging and the establishment of charging infrastructure, including the power distribution capacity to prevent overloading of circuits and the charging facility, as well as the information system to manage the energy distribution, and customer interface such as accounting and billing need to be in place.
- Grid monitoring and management: This application aims to enable the demand response and consumer energy efficiency. With demand-response, the balance of power supply and demand can be largely balanced. To this end, utilities, business, industrial, and residential customers have the feasibility to cut energy usage during the time of peak demand or when the power reliability is at risk. This application requires the dynamic pricing from the energy markets, the smart meters and real time usage data, the smart appliances, the home area networks and the networks for metering infrastructure, which will be illustrated next.
- Smart metering infrastructure: This application enables the AMI and provides customers real-time (or near real-time) pricing of electricity and can help utilities achieve necessary load reductions. It demands the communications hardware and software and associated system and data management software that creates a two-way network between advanced meters and utility business systems to enable the collection and the distribution of information to customers and other parties, such as the competitive retail supplier or the utility itself. Utilities also rely on AMI to implement residential demand response and to serve as the main mechanism for implementing dynamic pricing.

In order to support the Smart Grid applications discussed above, it is essential to add and integrate computing and communication technologies and services with existing electricity-delivery infrastructure. To this end, the ICT platform is required to provide the bidirectional flows of energy and two-way communication and control capabilities, enabling new functionalities and applications, including the smart metering for homes and businesses. Generally speaking, the platform for Smart Grid consists of the following:

- Connected electrical grid/ communication networks: Electrical grid needs to be integrated into an advanced, digital communication network infrastructure with two-way capabilities for communicating information, controlling equipment, and distributing energy. The use of a variety of public and private communication networks (wired or wireless) shall be integrated in Smart Grid.
- Distributed, intelligent, and secured grid control and management: On the top of connected electrical grid and communication network, the distributed and intelligent grid control and management plays a critical role to enable all key applications discussed above. To be specific, the energy intelligence, secured and QoS aware control and data planes need to be in place to meet the reliability, security, and QoS requirements of applications in Smart Grid. Because the Smart Grid will include networks from the diverse IT, telecommunications, and energy sectors, security shall also be required to ensure that a compromise in one network does not compromise security in other interconnected systems.

### 5.3.4. Architectural Overview for Smart Grid[149]

- Simplified domain model in ICT perspective

Figure 5-3-5 shows the simplified domain model based on NIST 7 domain model. This simplified domain model is composed of 5 domains as follows:

- Grid domain (bulk generation, distribution and transmission)
- Smart metering (AMI)
- Customer domain (smart appliances, electric vehicles, premises networks (Home/ Building/ Industrial Area Network))
- Communication network
- Service provider domain (markets, operators, service providers)

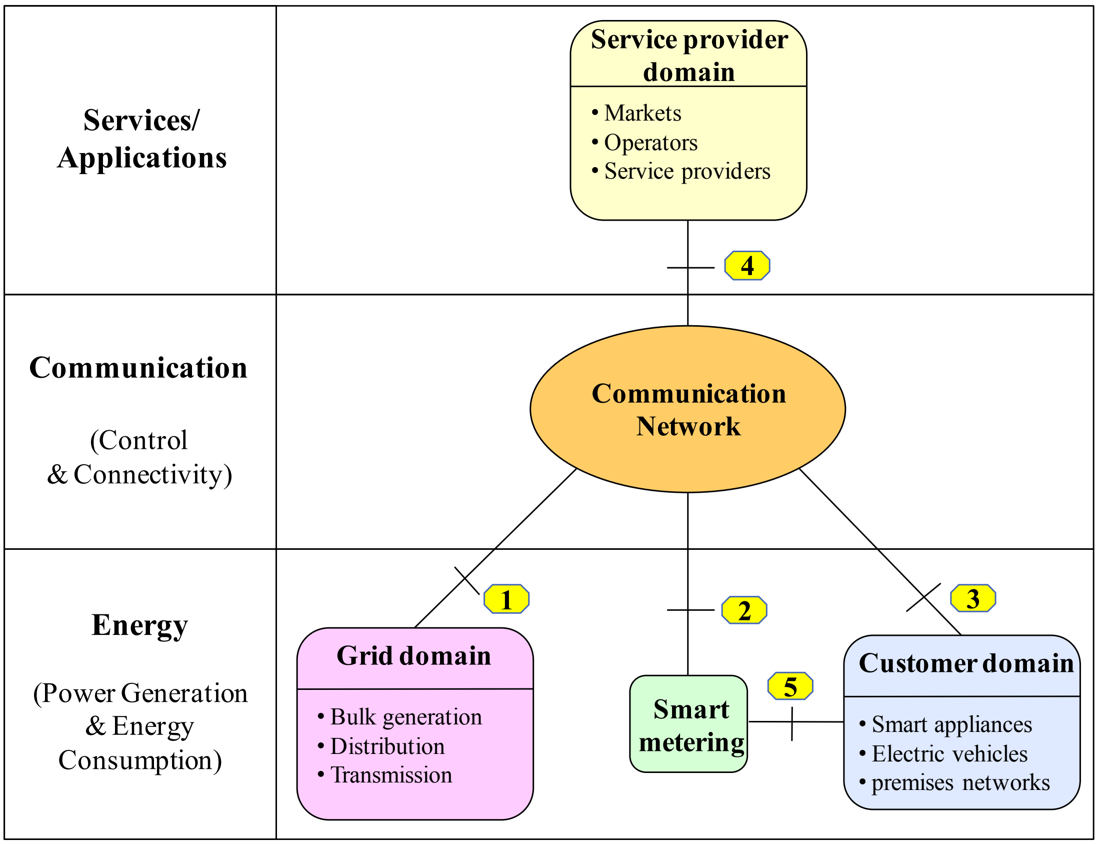



Figure 5-3-5. Simplified Smart Grid domain model in ICT perspective

Figure 5-3-5 shows five reference points from the network to other four domains, and between smart metering domain and customer domain. Samples functions at each of these reference points are listed below:

- Simplified reference architecture for Smart Grid

Figure 5-3-6 shows the simplified reference architecture which has 5 key domains from Figure 5-3-5. The five reference points are also highlighted in this figure. As we can see from Figure 7, the service provider domain, grid domain, customer domain, and smart metering are interconnected via a communication network. Using the customer domain as an example, all devices (e.g., electric-vehicle, customer EMS, electric storage) are connected via premises network (e.g., HAN or LAN). The premises network in customer domain also has the connection to communication

[149] ITU-T FG-Smart Deliverables

network cloud, connecting to other domains. As such, the customer domain EMS can interact with the metering/ billing / utility back office in the service provider domain. Using this figure, we can also see the other interactions between domains via the communication networks. For example, the field sensors in grid domain can interact with the SCADA in the operation of service provider domain for real-time remote sensing data collecting and control.

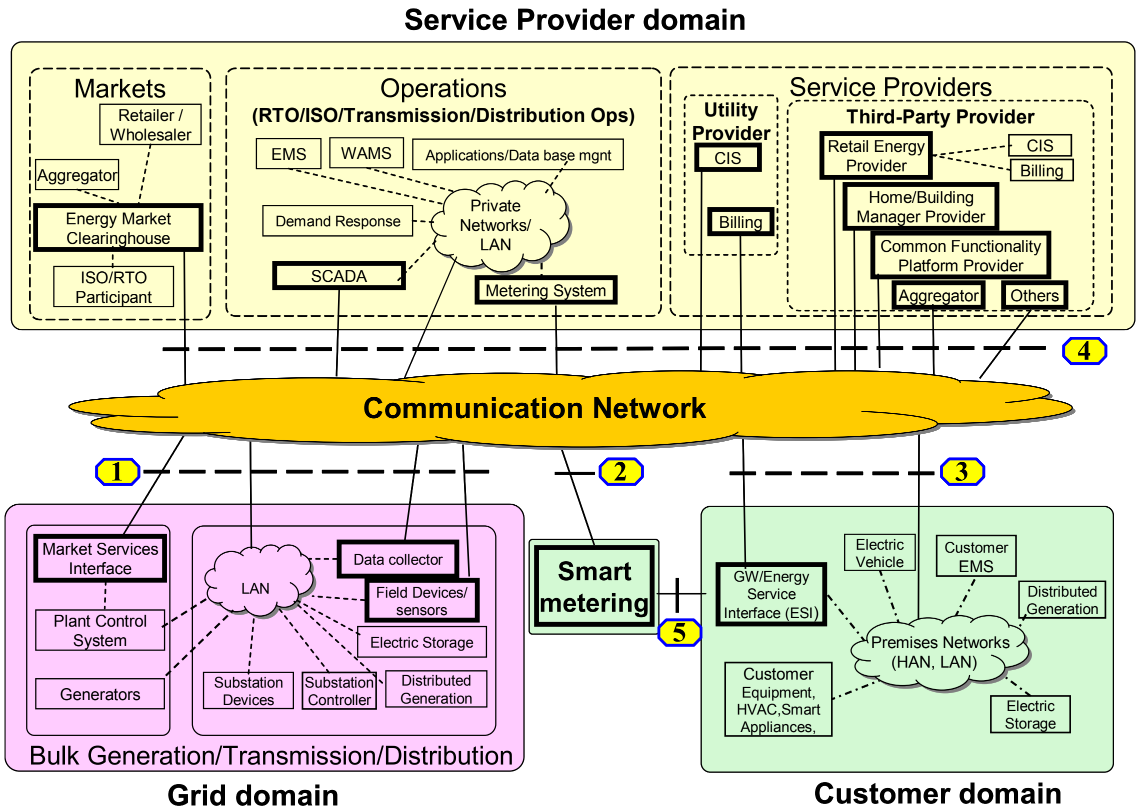


Figure 5-3-6. Simplified reference architecture for Smart Grid

Figure 5-3-6 represents a logical view of the smart grid system with a focus on communication interactions. The communications cloud represents the communications networks that connect logical devices in the smart grid. These communications networks may reside within a domain or cross-domain boundaries. The communications network may carry grid related data only or may be a general purpose network carrying grid data along with generic data. The choice of what type of network is needed to support a particular smart grid function shall be driven by the requirements of that function.

- Functional Model of Smart Grid

Smart Grid consists of a collection application/services/software/hardware as domains and elements of Smart Grid. This section provides a decomposition of functions in each of those functions which is shown Figure 5-3-7. These functions interact with each other to accomplish the goal of Smart Grid. This functional model provides an architectural framework for standard development.

For Smart Grid, the following functions should be addressed in each domain.

- Grid domain: power grid functions;
- Smart metering: smart metering functions;
- Customer domain: end-user functions;
- Communication network: telecommunication, including IP-based, network functions;
- Service provider domain: application functions.

In addition, management/security functions are required for all domains. Figure 5-3-7 shows relevant functions of Smart Grid and their relations between functions using a line with circles at the both ends.

The functional model in Figure 5-3-7 identifies the principle functional groups for Smart Grid, including the End-User Functions, the Application Functions, the Smart Metering Functions, the Energy Control Functions, the Power Grid Functions, the Network Functions, the Management Functions, and the Security Functions. Key functions within each functional group are shown within each box. The lines across the function boxes indicate data flows, and interactions between them.

The functions related to end users and end systems (e.g., power system devices) are shown on the left of Figure 5-3-7, while the core functions for Smart Grid, the Application Functions, the Network Functions, and the Energy Control Functions are shown in the middle column. A key focus of the Smart Grid, the Smart Metering Function is also shown in the middle. Two key function areas: (i) the Management and (ii) Security Functions have interaction with other functions and are shown on the right of Figure 3.

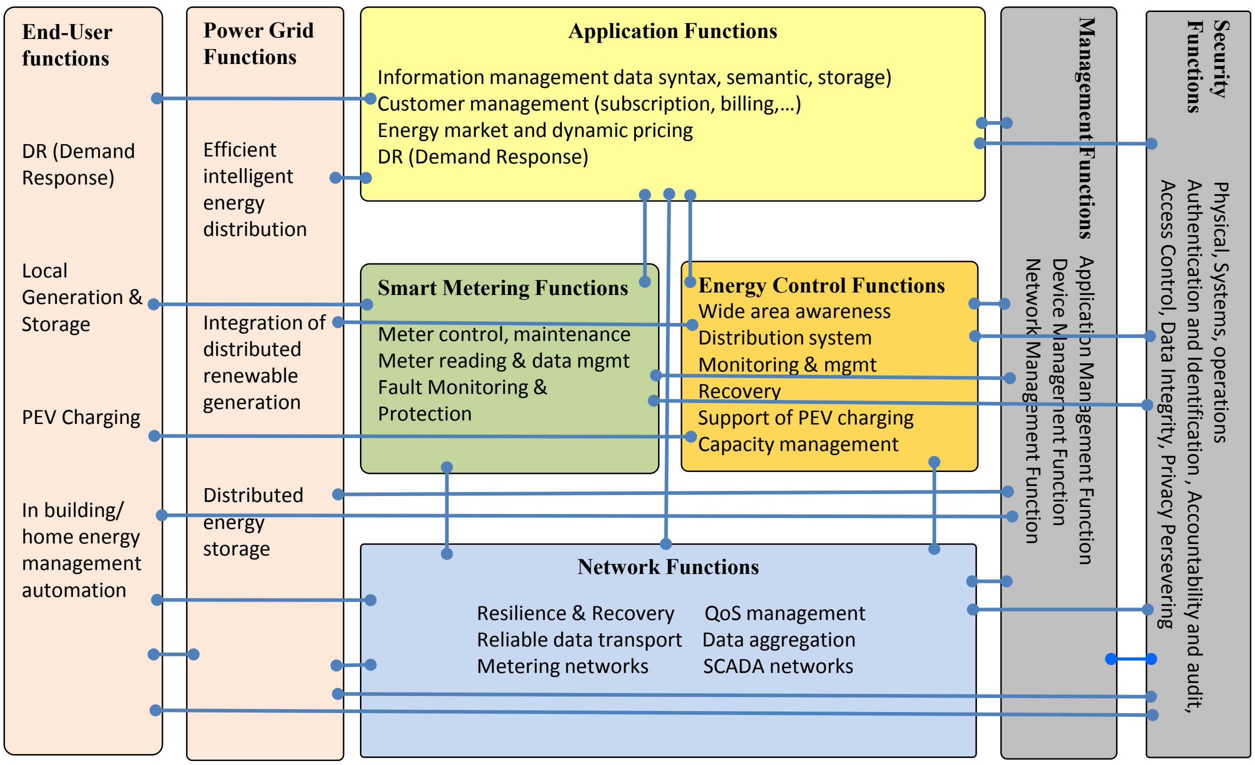


Figure 5-3-7. The Functional Model of Smart Grid

The key functions in each functional group are listed below:

- ***Power Grid Functions***: This function group performs functions to efficiently and intelligently distribute energy and integrate distributed renewable energy generation and distribution. It interacts with Application and Energy Control Functions through Network Functions, and interacts with End-User Functions for energy transmission.
- ***Network Functions***: This function group interacts with all other function groups to provide functions such as resilience and recovery, QoS management, reliable data transport, metering data transfer, data aggregation, real-time data transfer, and others:
  - Resilience and Recovery Function: This function provides the capability of effectively preventing and responding to disruptions due to cyber attacks, physical phenomena, software and hardware failures, upgrades and human mistakes;
  - QoS Management Function: This function is used to guarantee the performance (e.g., bandwidth, end-to-end delay, jitter, and others) of network. It provides the capabilities to differentiate and prioritize the data sent from a variety of devices (e.g., meters, appliances, substation, and others) thus enabling the delivery of information across the grid for different applications.

- ***Smart Metering Functions***: This function group encompasses the interaction with End-User Functions, Network Functions, Management Functions, and Security Functions groups. It performs functions to control and maintain metering equipment and to read meter data. It interacts with Application Functions group for establishing meter database and billing information and interacts with Network Functions group for meter data aggregation and transportation; it may interact with End-User Functions through gateways and home networks. This function group also enables the real-time monitoring and protection via effective event or alarm reporting and processing.
- ***Energy Control Functions***: This function group performs functions to monitor and manage distributed energy resources and support services such as PEV charging, and to manage energy capacity planning. It interacts with End-User Functions and Application Functions group through Network Functions.
- ***End-User Functions***: This function group consists of energy Demand Response (DR), home/ building energy management and automation, local energy generation and storage, and PEV charging functions. It interacts with DR application for dynamic pricing information, controls energy usage of home appliances and in-building equipment. It also interacts with Energy Control Functions for distribution capacity management and two-way energy transmission.
- ***Application Functions***: This function group consists of functions for application system information management (e.g., data syntax, semantic, and storage), customer information management (e.g., billing, user subscription), energy market and dynamic pricing as well as energy DR management and control. This function group interacts with End-User Functions, Smart Metering Functions, Energy Control Functions, Management Functions, and Security Functions groups. This function may interact with End-User function, Energy control function and Power grid function to manage environmental parameters.
- ***Management Functions***: This function group consists of functions for management of systems in all function blocks. This function group interacts with all other function groups and covers various system management, including application management, device management, and network management:
  - Application Management Function: This function provides the functions to help the operator to manage the key aspects of applications. It monitors various applications and helps application providers to ensure that their applications meet end-user's expectations;
  - Device Management Function: This function enables the communication with a vast array of devices in the field and substations, whether heterogeneous or homogeneous. The device management provides an efficient way to normalize and transmit data to and from these devices;
  - Network Management Function: This function provides management of communications network to ensure availability and stability. It is also responsible for keeping track of network resources and how they are assigned, configuring resources in the network to support a given service, and adjusting configuration parameters in the network for better quality.
- ***Security Functions***: This function group interacts with all other function groups in terms of physical security, system security, and operation security. This function group covers various security aspects and the examples of applications are described below:
  - Identification and Authentication Function: This function is the process of verifying the identity of a user, process, or a device, as a prerequisite for granting access to resources in a Smart Grid system;
  - Audit and Accountability Function: This function enables the review and the examination of the information record and activities related to Smart Grid to determine the adequacy of security requirements and to ensure compliance with the established security policy and procedures;
  - Access Control Function: This function ensures that only authorized personnel or users have access to use various utilities and services in the grid system;
  - Data Integrity Function: The function is responsible for data integrity in Smart Grid via cryptography and validation mechanisms;
  - Privacy Preserving Function: This function is designed to provide the privacy considerations with respect to the Smart Grid.

A more detailed requirements and description of Security Functions can be found in NISTIR 7628 - Guidelines for Smart Grid Cyber Security[150].

---

[150] NIST Interagency Report (NISTIR) 7628, "Guidelines for Smart Grid Cyber Security: Vol.2, Privacy and the Smart Grid," August 2010.

### 5.3.5. Standardization for Smart Grid

- Smart Grid Standards from International Standard Developing Organizations (SDOs)

From the analysis in previous sections on key areas of ICT for Smart Grid and Smart Grid functional models, we can classify Smart Grid standards into several categories as shown below:

- ***Grid management***: standards for control and management of power generation, transmission, and distribution, including the functions and operations of components for these systems such as sensors, controllers, and meters;
- ***Information management***: standards for exchange of data between the Smart Grid subsystems, components, and applications or services, including syntax and semantics rules, timing, frequency, and volume of information to be exchanged;
- ***Communications and networking***: standards for communication network to transfer information for Smart Grid functions, including the transmission media and transport functions;
- ***Applications and services***: standards for invocation, termination, recovery of Smart Grid applications and services;
- ***Security and privacy***: standards related to the physical security and cyber security of Smart Grid systems, and the privacy of data generated and collected.

There are many international SDOs, besides the ITU-T which is the focus of this article, that have developed and are developing standards related to Smart Grid. These include IEC, IEEE, and IETF. There are also regional or national SDOs that focus on regional or national needs. Furthermore there are also public consortia for development specifications and implementation agreements on specific topics.

The U.S. Congress recognized having interoperable standards is a major issue for the future development of Smart Grid, and it tasked the NIST under the Energy Independence and Security Act (EISA) of 2007 to coordinate development of standards to achieve interoperability of Smart Grid devices and systems. In the NIST Framework and Roadmap for Smart Grid Interoperability Standards[151], a set of standards applicable to the Smart Grid, and standards need further harmonization were identified. NIST established the Smart Grid Interoperability Panel (SGIP)[152] to coordinate with all SDOs on the harmonization and development of smart grid standards. Similarly the European Commission issued a Smart Grid mandate M/490[153] for the European SDOs to develop or update a set of consistent standards that will achieve interoperability and will enable or facilitate the implementation in Europe[154].

[151] National Institute of Standards and Technology, "NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 2.0," February 2012.

[152] NIST Smart Grid Collaboration Wiki Smart Grid Interoperability Panel (SGIP) Site, [Online] Available: http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/WebHome.

[153] *Smart Grid Mandate – Standardization Mandate to European Standardization Organizations (ESOs) to support European Smart Grid deployment*, M/490 EN, March 2011.

[154] *European Smart Grids Technology Platform: Strategic Deployment Document for Europe's Electricity Networks of the Future*– final version – 20 April 2010.

Smart Grid related ITU-T documents

| No | Group | Document title | Scope of document | Status |
|---|---|---|---|---|
| **1** | FG-Smart | **FG-Smart** Deliverable Smart Grid Overview | This deliverable provides an overview of Smart Grid.<br>The objective of this deliverable is to understand key concepts and objectives for Smart Grid and identify architectural models and required capabilities in the Information and Communication Technology (ICT) perspective. More specifically, this Deliverable covers the following:<br>• Definition of Smart Grid;<br>• Objectives of Smart Grid;<br>• Conceptual model and reference architecture of Smart Grid;<br>• Fundamental characteristics of Smart Grid;<br>• Roles and key areas of ICT for Smart Grid;<br>• Architecture overview for Smart Grid; and<br>• Required capabilities for Smart Grid. | Technical Report (12/2011) |
| **2** | FG-Smart | **FG-Smart** Deliverable Use Cases for Smart Grid | This deliverable describes use cases for smart grid.<br>The objective of this deliverable is to analyse several use cases for smart grid in the ICT perspective and identify requirements and architectural considerations. | Technical Report (12/2011) |
| **3** | FG-Smart | **FG-Smart** Deliverable Requirements of communication for smart grid | This deliverable document specifies requirements of Smart Grid based on the three different areas defined in overview deliverable including Smart Grid Services/Applications area, Communication area and Physical Equipment area. | Technical Report (12/2011) |
| **4** | FG-Smart | **FG-Smart** Deliverable Smart Grid Architecture | This deliverable document describes architecture for smart grid. First, this document describes the reference architecture, including the simplified domain model in ICT perspective and mapped domain model based on NIST smart grid Interoperability framework. Second, the smart grid functional architecture and two representative applications, namely "smart metering and load control" and "energy distribution and management" are introduced. Lastly, the deployment models of smart grid are introduced and they consist of the networking and communication techniques, network architecture, and deployment model and implementation. | Technical Report (12/2011) |
| **5** | FG-Smart | **FG-Smart** Deliverable Smart Grid Terminology | This Deliverable collects the key terms which are closely related with grid and appeared in the deliverables on Overview, Use Cases, Requirements and Architecture. The corresponding definitions of these key terms are also provided in this deliverable. | Technical Report (12/2011) |

| | | | | |
|---|---|---|---|---|
| **6** | ITU-T SG13 Q11 | **Y.HEMS-arch** Requirements and architecture of home energy management system and home network services | This draft Recommendation provides the requirements and architecture of home energy management system (HEMS) and home network (HN) services. The HEMS which would realize energy-efficiency and reduction of the energy consumption. It is realized by monitoring and controlling the devices connected to the home network (HN) such as home appliances, storage batteries and sensors from the HEMS application on the Internet. This draft Recommendation covers the followings.<br>• Overview<br>• Requirements for the key components in the architecture<br>• Reference Architecture<br>• Functional architecture<br>• Security<br>The HEMS service is one of the HN services. Since it has been widely known what it is, the requirements and architecture of the HN services are described mainly with the HEMS service in this Recommendation. The architecture iscould also be applied to the other HN services such as the home security and the healthcare. The HN services can cooperate with other Internet applications and therefore expand to various services with controlling the home devices. | Under Study |
| **7** | ITU-T SG13 Q11 | **Y.meg** Framework of micro energy grid | This draft Recommendation provides the framework of micro energy grid for interconnected local generation and distribution. After identifying key features from the concepts of micro energy grid, this draft Recommendation specifies requirements and capabilities in terms of networks and services as well as users considering distributed energy sources. Then, this draft Recommendation provides architectural overview including the domain model as well as the functional architecture and deployment models. Finally detailed operations of control and management services for micro energy gird are described.<br>Therefore, this draft Recommendation covers the following:<br>• Features of micro energy grid<br>• Requirements and capabilities for micro energy grid<br>• Architectural framework of micro energy grid<br>• Communication networks and deployment models from end user networks perspective<br>• Control and management services for micro energy grid from use case analysis | Under Study |
| **8** | ITU-T SG15 Q15 | **G.9955** Narrowband OFDM Power Line Communication Transceivers – | This Recommendation contains the physical layer specification for narrowband OFDM power line communications transceivers for communications via alternating current and direct current electric power lines over frequencies below 500 kHz. This Recommendation supports indoor and outdoor communications over low voltage lines, medium voltage lines, through transformer low-voltage to medium-voltage and through transformer medium-voltage to low-voltage power lines in both urban and in long distance rural communications. This | Published (12/2011) |

| | | | | |
|---|---|---|---|---|
| | | Physical Layer Specification | Recommendation addresses grid to utility meter applications, advanced metering infrastructure (AMI), and other Smart Grid applications such as charging of electric vehicle, home automation, and home area networking (HAN) communications scenarios. | |
| **9** | ITU-T SG15 Q15 | **G.9956** Narrowband OFDM Power Line Communication Transceivers – Data Link Layer Specification | This Recommendation contains the data link layer specification for narrowband OFDM power line communications transceivers for communications via alternating current and direct current electric power lines over frequencies below 500 kHz. This Recommendation supports indoor and outdoor communications over low voltage lines, medium voltage lines, through transformer low-voltage to medium-voltage and through transformer medium-voltage to low-voltage power lines in both urban and in long distance rural communications. This Recommendation addresses grid to utility meter applications, advanced metering infrastructure (AMI), and other Smart Grid applications such as charging of electric vehicles, home automation, and home area networking (HAN) communications scenarios. | Published (11/2011) |
| **10** | ITU-T SG15 Q15 | **G.9901** Narrow-band OFDM power line communication transceivers - Power spectral density specification | This Recommendation specifies the control parameters that determine spectral content, power spectral density (PSD) mask requirements, a set of tools to support the reduction of the transmit PSD, the means to measure this PSD for the transmission over power line wiring, as well as the allowable total transmit power into a specified termination impedance. It complements the system architecture, physical layer (PHY), and data link layer (DLL) specifications in Recommendations ITU T G.9902 (G.hnem), ITU-T G.9903 (G3-PLC) and ITU-T G.9904 (PRIME). | Published (04/2014) |
| **11** | ITU-T SG15 Q15 | **G.9902** Narrow-band OFDM power line communication transceivers for ITU-T G.hnem networks | Recommendation ITU-T G.9902 contains the physical layer (PHY) and the data link layer (DLL) specifications for the ITU-T G.9902 narrowband orthogonal frequency division multiplexing (OFDM) power line communication transceivers operating over alternating current and direct current electric power lines over frequencies below 500 kHz. This Recommendation supports indoor and outdoor communications over low voltage-lines, medium-voltage lines, through transformer low-voltage to medium-voltage and through transformer medium-voltage to low-voltage power lines in both urban and long-distance rural communications. This Recommendation addresses grid to utility meter applications, advanced metering infrastructure (AMI) and other 'Smart Grid' applications such as the charging of electric vehicles, home automation and home area network (HAN) communications scenarios. This Recommendation does not contain the control parameters that determine spectral content, power spectral density (PSD) mask requirements and the set of tools to support a reduction of the transmit PSD; all of which are detailed in [ITU-T G.9901]. | Published (10/2012) |
| **12** | ITU-T SG15 Q15 | **G.9903** | Recommendation ITU T G.9903 contains the physical layer (PHY) and data link layer (DLL) specification for the G3-PLC narrowband orthogonal frequency division multiplexing | Published (02/2014) |

| | | | | |
|---|---|---|---|---|
| | | Narrow-band OFDM power line communication transceivers for G3-PLC networks | (OFDM) power line communication transceivers for communications via alternating current and direct current electric power lines over frequencies below 500 kHz. This Recommendation supports indoor and outdoor communications over low-voltage lines, medium-voltage lines, through transformer low-voltage to medium-voltage and through transformer medium-voltage to low-voltage power lines in both urban and long distance rural communications. This Recommendation addresses grid to utility meter applications, advanced metering infrastructure (AMI), and other 'Smart Grid' applications such as the charging of electric vehicles, home automation and home area networking (HAN) communications scenarios.<br>This Recommendation does not contain the control parameters that determine spectral content, power spectral density (PSD) mask requirements and the set of tools to support a reduction of the transmit PSD; all of which are detailed in Recommendation ITU-T G.9901.<br>The ITU-T would like to acknowledge the IEEE Std 1901.2(TM)-2013 for the information related to some features that are specified in this Recommendation (ADMI, AC phase detection, and some aspects of Reed-Solomon encoding and full block interleaving) [b-IEEE 1901.2-2013]. | |
| **13** | ITU-T SG15 Q15 | **G.9904**<br>Narrow-band OFDM power line communication transceivers for PRIME networks | This Recommendation contains the physical layer (PHY) and data link layer (DLL) specification for PRIME narrowband orthogonal frequency division multiplexing (OFDM) power line communication transceivers for communications via alternating current and direct current electric power lines over frequencies below 500 kHz. This Recommendation supports indoor and outdoor communications over low-voltage lines, medium-voltage lines, through transformer low-voltage to medium-voltage and through transformer medium-voltage to low-voltage power lines in both urban and in long distance rural communications. This Recommendation addresses grid to utility meter applications, advanced metering infrastructure (AMI), and other 'Smart Grid' applications such as the charging of electric vehicles, home automation and home area networking (HAN) communications scenarios.<br>This Recommendation removes the control parameters that determine spectral content, power spectral density (PSD) mask requirements, and the set of tools to support reduction of the transmit PSD, all of which have been moved to [ITU-T G.9901]. | Published (10/2012) |
| **14** | ITU-T SG15 Q15 | **G.9905**<br>Centralized metric based source routing | Recommendation ITU-T G.9905 specifies centralized metric based source routing (CMSR), a proactive, layer 2 multi-hop routing protocol. CMSR is a proactive routing protocol which can find and maintain reliable routes considering the link quality of both directions. The routing control packet overhead of CMSR is quite low compared to existing proactive routing protocols such as optimized link state routing (OLSR), so that it can be applied for large-scale networks even on narrow band power line communication (PLC) networks. | Published (08/2013) |

| | | | | |
|---|---|---|---|---|
| **15** | ITU-T SG15 Q15 | **G.9959** Short range narrowband digital radiocommunication transceivers – PHY & MAC layer specifications | This Recommendation contains the MAC/PHY layer specification for short range narrow-band digital radiocommunication transceivers. This Recommendation is a joint work of ITU-R and ITU T, each contributing material from their respective remits. This Recommendation contains the non-radio (frequency) related aspects of the radiocommunication transceiver. The Recommendation specifies sub 1 GHz transceivers which shall be interoperable with transceivers complying with Annex A of this Recommendation. | Published (02/2012) |

# 6. Comparisons

## 6.1 Mobile broadband access networks

**Technical comparison**[155]
The 4G (e.g., LTE and WiMAX) currently being marketed can theoretically deliver a peak of up to 128 Mbit/sec downstream under perfect conditions for an ideally situated stationary user. The real IMT-Advanced 4G will provide 100 Mbit/sec downstream even for users moving in high-speed vehicles and 1Gbit/sec for stationary users.
As a major shift away from mixed voice-and-data networks, IMT-Advanced with full IP is expecting the following characteristics compared to previous technologies:

- Reliable data rates of 1GB/sec for stationary connections, and 100Mbit/sec for mobile
- High definition, high quality multimedia
- Smooth, seamless handover between networks and among cells
- Full IP-based packet-switched networks, compatible with IPv6
- Advanced automatic network asset allocation, and scalability

Table 6-1-1 shows the evolution and migration of wireless-data technologies from EDGE to LTE, as well as the evolution of underlying wireless approaches. Progress in 3GPP has occurred in multiple phases, first with EDGE, and then UMTS, followed by today's enhanced 3G capabilities such as HSPA, HSPA+, and now, LTE, which itself is evolving to LTE-Advanced. Meanwhile, underlying approaches have evolved from Time Division Multiple Access (TDMA) to CDMA, and now from CDMA to OFDMA, which is the basis of LTE.

Table 6-1-1. Characteristics of 3GPP Technologies

| Technology | Type | Characteristics |
|---|---|---|
| GSM | TDMA | Most widely deployed cellular technology in the world. Provide voice and data service via GPRS/EDGE |
| EDGE | TDMA | Data service for GSM networks. An enhancement to original GSM data service called GPRS. |
| Evolved EDGE | TDMS | Advanced version of EDGE that can double and eventually quadruple throughout rates, halve latency and increase spectral efficiency |
| UMTS | CDMA | 3G technology providing voice and data capabilities. Current deployments implement HSPA for data service. |
| HSPA | CDMA | Data service for UMTS networks. An enhancement to original UMTS data service. |
| HSPA+ | CDMA | Evolution of HSPA in various stages to increase throughput and capacity and to lower latency. |
| LTE | OFDMA | New radio interface that can use wide radio channels and deliver extremely high throughput rates. All communications handled in IP domain. |
| LTE Advance | OFDMA | Advanced version of LTE designed to meet IMT-advance requirements |

More competitive summary, Table 6-1-2 summarizes key technological features of three different technology groups (e.g., EDGE/HSPA/LTE, CDMA2000, WiMAX).

155 Paul B. Wordman , "4G IMT Advanced, LTE, WiMAX vs 3G Speed – Executive Summary", Jan. 2012. http://blog.parts-people.com/2012/01/27/4g-imt-advanced-lte-wimax-vs-3g-speed-executive-summary/
RYSAVY research "Transition to 4G 3GPP broadband evolution to IMT-advanced" Sept. 2010.

Table 6-1-2. Comparison of major mobile broadband access networks

| Technology | EDGE/HSPA/LTE | CDMA2000 | WiMAX |
|---|---|---|---|
| **Subscribers** | Over 4.4 billion | 518 million; slower growth expected than GSM-HSPA | 61 million anticipated by 2014 |
| **Maturity** | Extremely mature | Extremely mature | Emerging |
| **Adoption** | Cellular operators globally | Cellular operators globally | Limited to data |
| **Coverage/Footprint** | Global | Global with the general exception of Western Europe | Limited |
| **Development** | Fewer cell sites required at 700 and 850 MHz | Fewer cell sites required at 700 and 850 MHz | Many more cell sites required at 2.5 GHz |
| **Devices** | Broad selection of GSM/EDGE/UMTS/HSPA devices | Broad selection of 1xRTT/EV-DO devices | Initial devices emphasize data |
| **Radio Technology** | Highly optimized TDMA for EDGE, highly optimized CDMA for HSPA, highly optimized OFMA for LTE | Highly optimized CDMA for Rev 0/A/B | Optimized OFDMA in Release 1.0. More optimized in Release 1.5 |
| **Spectrum Efficiency** | Very high with HSPA, matches OFMA approaches in 5 MHz with HSPA+ | Very high with EV-DO Rev A/B | Very high, but not higher than HSPA+ for Release 1.0, and not higher than LTE for Release 1.5 |
| **Throughput Capabilities** | Peak downlink use-achievable rates of 4 Mbps with achievable rates of over 8 Mbps with HSPA+ | Peak downlink user-achievable rates of over 1.5 Mbps, with significantly higher rates in the future | 3 to 6 Mbps typical rates with bursts to 10 Mbps |
| **Voice Capability** | Extremely efficient circuit-voice available; smoothest migration to VoIP of any technology | Extremely efficient circuit-voice available. EV-DO radio channels with VoIP cannot support circuit-voice users | Relatively inefficient VoIP initially; more efficient in later stages, but lower than LTE<br>Voice coverage will be much more limited than cellular |
| **Simultaneous Voice and Data** | Available with GSM and UMTS | Not available today Available with VoIP and future devices | Potentially available, through initial services will emphasize data |
| **Efficient Spectrum Usage** | Entire UMTS radio channel available for any mix of voice and high speed data | Radio channel limited to either voice/medium speed data or high speed data only | Currently only efficient for data centric networks |

Based on different characteristics of mobile broadband access technologies, Figure 6-1-1 illustrates evolution of different types of system and their downlink and uplink speeds.

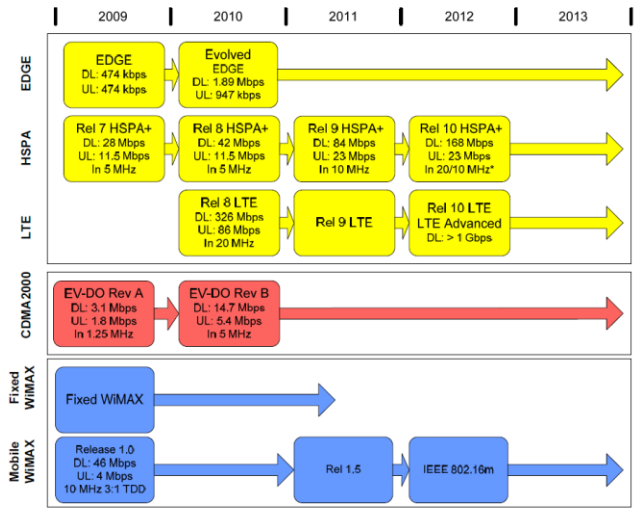


Figure 6-1-1. Evolution of TDMA, CDMA, and OFDMA Systems

**Financial considerations**
From Figure 6-1-2, we can estimate that 3G subscribers on networks will number in the many hundreds of millions by the end of this decade, whereas subscribers to emerging wireless technologies, such as WiMAX, will number in the tens of millions.

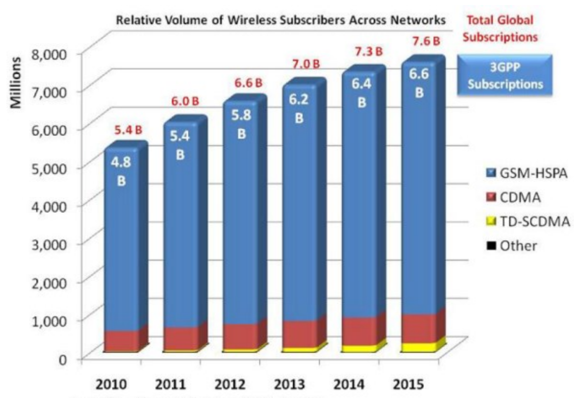


Figure 6-1-2. Relative volume of subscribers across mobile broadband access network technologies

Although proponents for technologies such as mobile WiMAX point to lower costs for their alternatives, there doesn't seem to be any inherent cost advantage—even on an equal volume basis. And when factoring in the lower volumes, any real-world cost advantage is debatable.
From a deployment point of view, the type of technology used (for example, HSPA versus WiMAX) only applies to the software supported by the digital cards at the base station. This cost, however, is only a small fraction of the base station cost with the balance covering antennas, power amplifiers, cables, racks, RF cards. As for the rest of the network including construction, backhaul, and core-network components, costs are similar regardless of Radio Access Network (RAN) technology. Spectrum costs for each technology can differ greatly depending on a country's regulations and the spectrum band. As a general

rule in most parts of the world, spectrum sold at 3.5 GHz will cost much less than spectrum sold at 850 MHz (all other things being equal).
As for UMTS-HSPA versus CDMA2000, higher deployment—by a factor of five—could translate to significant cost savings. For example, research and development amortization results in a four-to-one difference in base station costs. Similarly, just as GSM handsets are considered much less expensive than 1xRTT handsets, UMTS-HSPA wholesale terminal prices could be the market leader in low-cost or mass-market 3G terminals. Even LTE is on the road to a robust wireless ecosystem and significant economies of scale.

## 6.2 Fixed broadband access networks

**Technical comparison**[156]
Gigabit-capable passive optical networks (GPON) and Ethernet passive optical networks (EPON) are two standards that open the door to new opportunities both for vendors and operators. Major vendors have added PON technology to their broadband access portfolios, and operators around the world have shown considerable interest in deploying this technology in combination with VDSL (fiber to the cabinet, FTTC) or as residential access (fiber to the home, FTTH). The three major PON standards are BPON (broadband PON), GPON, and EPON. BPON and its successor GPON are ITU-T recommendations sponsored by FSAN, a vendor and operator committee. EPON is an IEEE option developed by the IEEE Ethernet in the First Mile (EFM) initiative. Given that operators are driving GPON standardization via FSAN, the GPON standard reflects operator needs more directly than does EPON. Although all three systems work on the same principle, there are several differences between them as shown in Table 6-2-1.

Table 6-2-1. Major PON technologies and properties

| Characteristics | EPON | BPON | GPON | XG-PON | NG-PON2 |
|---|---|---|---|---|---|
| **Standard** | IEEE 802.3ah | ITU-T G.983 | ITU-T G.984 | ITU-T G987 | ITU-T G.989 |
| **Protocol** | Ethernet | ATM | Ethernet, TDM | | |
| **Rate (Mbps)** | 1250 down / 1250 up, 8b10b-encoded | 622 down, 155 up | 2488 down, 1244 up | 10 Gbps (down) | 40 Gbps (down) |
| **Span (km)** | 10 | 20 | 20 | | |
| **Split-ratio** | 16 | 32 | 64 | | |

156 Elmar Trojer et al, "Current and next-generation PONs: A technical overview of present and future PON technology," Ericsson Review No. 2, 2008

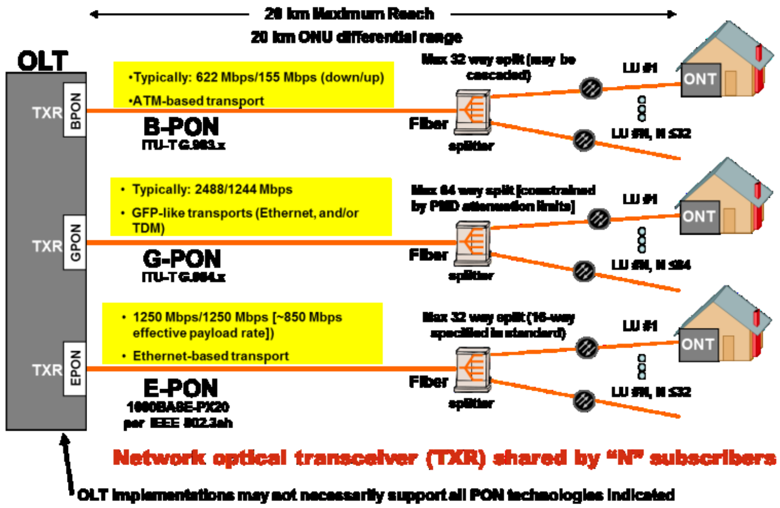



Figure 6-2-1. TDM PON architecture and technologies

As shown in Figure 6-2-1, the vast majority of PON systems deployed today are TDM-based PON systems (i.e., B-PON, E-PON, and G-PON). They almost exclusively operate on a single fiber, with WDM used to provide bi-directional transmission. A third wavelength in the downstream is sometimes used for broadcast video services.

On the other hand, WDM-PON is very limited deployed mainly in Korea. Costs of WDM-PON in delivering mass market dedicated wavelength services are still higher high relative to TDM-PON. WDM and hybrid WDM-PONs are expected to play a greater role in next generation PON systems in the future.

**Financial considerations**[157]

As PON technology advances from 1G to 10G and even higher rates, operators are gearing up for a future user bandwidth requirement to 100M and even 1G. The mainstream bandwidth requirement is targeted as 100M for residential users and 1G for commercial users in the future.

10G PON supports a maximum 10G downstream rate, which can accommodate the access requirements of future users. On the issue of PON cost, however, 10G PON will cost 3–5 times of GPON. Considering the enormous network deployment cost, FTTB/C scenarios are the initial applications of 10G PON, where cost can be shared among more users. ONU cost takes up about 60% of the total cost of FTTH equipment. Therefore, the large scale deployment of 10G PON in the FTTH scenario depends on the development of the chips and optical components for 10G PON. It is anticipated that, in 2015, the cost of 10G PON products will be approximately the same as that of the current GPON products. Therefore, by 2015, operators can select 10G PON to increase the bandwidth of residential users to 100M and commercial users to 1G as Figure 6-2-2 summarizes.

157 "Next Generation PON Evolution" Huawei, 2010

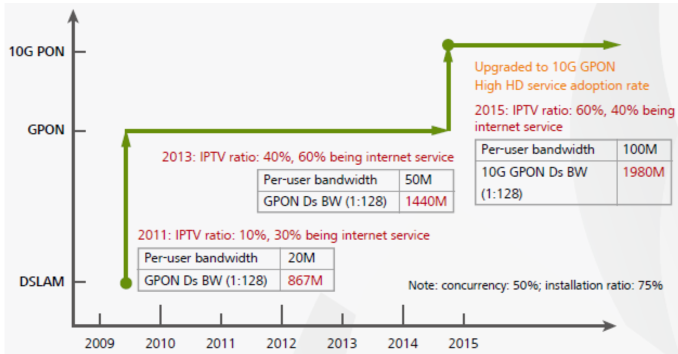


Figure 6-2-2 Roadmap of rate-rise for FTTH

Component vendors are at the first stage of the industry chain. They develop ASIC chips and optical transceivers only after NG PON standards are released. The ASIC chips and optical transceivers are the core of an NG PON system. Optical components and PON chipset account for over 60% of the total ONT cost. Meanwhile, the cost of current 10G PON optical components and chipset are 30–50 times higher than those of GPON's. Therefore, large scale application of ONT products relies on cost reduction. Multi-Dwelling Unit (MDU), which is for FTTB/C, has a different cost distribution in ONT. The cost of the optical transceiver and PON chipset of an MDU take up only about 25% of the total cost. At the same time, a single FTTB/C MDU usually services over 24 users and the per-user cost is lower. The cost of MDU optical components and PON chipsets will be affordable if falling down to 4–6 times of current GPON components.

In terms of network maintenance and management, the unified network management system (NMS) is required to manage PON ports and 10G PON ports at the same time with higher O&M efficiency and lower O&M expenditure. To sum up, large capacities, shared platforms, and unified network management systems will be the trends in 10G PON equipment developments that vendors are striving to fulfill.

## 6.3 Core networks

**Technical comparison**[158]

"Decoupling of service provision from transport operation" is one of key features of the NGN core network. Before the NGN, service provisions are tightly coupled with underline transport technologies. Another crucial point is the adoption of open and standardized interfaces between each functional level in order to allow third parties to develop and create services independent of the network. The following Table 6-3-1 shows the comparison between the NGN core network and the legacy core network.

Table 6-3-1. Comparison between the NGN core network and the legacy core network

| | **Non-NGN core network** | **NGN core network** |
|---|---|---|
| **Service provisions** | Service provisions tightly coupled with underline transport. | Decoupling of service provision from transport operation. |
| **Transport Technology** | Various transmission technologies | IP transport technology. |
| **QoS support** | It depends on the transport QoS scheme and there is no guaranteed QoS. | NGN core provides various classes of QoS. |
| **Mobility support** | Mobility is not mandatory capability. | NGN core supports FMC and heterogeneous mobility. |

[158] Series Y.2000: Next Generation Networks, "Migration scenarios from legacy networks to NGN in developing countries," Mar. 1, 2013

.

**Financial considerations**[159]

NGN core network can reduce the overall cost level by converging various type of services onto a single network infrastructure. At the same time, the capacity and processing power of modern network equipment can result in increased economies of scale and in innovation in services and in packaged retail propositions. The greater economies of scale in NGNs are likely to increase the challenges in promoting effective competition in the provision of services solely reliant on core infrastructure.

Therefore, NGN core technology is expected to save costs. The cost structure of NGN core networks is likely to contain a relatively high proportion of costs common to all services carried by the network, and a relatively low proportion of costs directly driven by the volume of each service.

## 6.4 Home networks

**Technical comparison**[160]

In order to deploy home network, service providers need to select a proper technology among various home network technologies in consideration of service requirements. Generally speaking, a common problem in wired topologies is that they are difficult to be done in existing homes and have constrain to move nodes from one place to another. For these reason, wireless home networks are getting more popular. The following Table 6-4-1 shows the comparison among the various networking technologies in terms of speed and range.

159 Adapted from ERG (08) 26 final NGN IP-IC CS 081016, "ERG Common Statement on Regulatory Principles of IP-IC/NGN Core -A work program towards a Common Position"

160 Compiled from: Munish Mangal and Nishant Omar, "Picking the right technologies for your home network design," Embedded.com, Nov. 2009.

Table 6-4-1. Comparison among the various networking technologies

| Wired/Wireless | Technology | Speed | Range |
|---|---|---|---|
| Wired | Ethernet 10/100 | 100Mbps | Very Good |
| | Phone Line 2.0 | 10Mpbs | Very Good |
| | Gigabit Ethernet | 1,000Mbps | Very Good |
| | Power Line | 14Mbps | Very Good |
| Wireless | 802.11g | 22/54Mbps | Poor |
| | Bluetooth | 1.5Mbps | Bad |
| | HomeRF 2.0 | 10Mbps | Good |
| | 802.11b | 11Mbps | Good |
| | 802.11a | 52/72Mbps | Good |
| | 802.15.4 (Zigbee) | 2Mbps | Very Good |

**Financial considerations**[161]

Service providers want to reduce the cost of building a home network. It takes many expenses to configure or setup the wired home network because cabling installation and maintenance requires much money. As compared to the wired home network, it is relatively easier to setup a wireless home network. On the other hand, wireless coverage is not guaranteed as it depends upon the construction and density of a home's walls and is vulnerable to interference. While the ability to rely upon a single network technology would be ideal, it could not be realistic for many cases in consideration of wireless coverage and cabling cost of a wired network. To meet the needs of today's consumers and service providers, a hybrid network which combines a wired home network and a wireless home network could be a good solution It also cloud increase the confidence with which service providers can reliably supply services through complementary coverage.

## 6.5 IPTV

**Technical comparison**[162]

There are several approaches to deploy IPTV for service providers. The representative IPTV deployment could be classified into Non-NGN-based IPTV and NGN/IMS-based IPTV. The following Table 6-5-1 shows the comparison between them.

Table 6-5-1. Comparison between non-NGN based IPTV and NGN/IMS based IPTV

| General characteristics | Non-NGN based IPTV architecture | NGN/IMS based IPTV architecture |
|---|---|---|
| **Standardization** | Vendor- & industry-driven | This standards is in focus of standard bodies (ETSI, ITU-T) |
| **Modularity and open protocols** | Low, proprietary protocols | Higher, standardized open protocols |
| **Media processing and service control separation** | Functions are highly integrated in network elements and middleware | Separated service control from delivery and media control |
| **Control functions** | Stream delivery control oriented | Session control oriented streams |

161 Stephen Palm, Broadcom Corporation, "Uniting wired and wireless home networking" , "Wired Vs Wireless home networks," wifinotes.com

162 Adapted from Eugen Mikoczy, "NGN based IPTV," 3rd International ngnlab.eu workshop on NGN, Delft, Nederland, Nov. 2012.

| | | |
|---|---|---|
| **Transport control functions** | Missing specialized elements to effect from application the transport control | Elements in the architecture for providing QoS (RACF) |
| **Application & Services** | less limited to legacy IPTV | broadcasting & communication convergence |
| **Service Capabilities and Enablers** | No common service capabilities or service enablers | Shareable service enablers to support complex applications |
| **Service integration** | Limited to each IPTV service platform | Possible across service layer of IMS based NGN architecture |
| **End devices** | Limited number of STBs | More standardized devices |

**Financial considerations**[163]
IPTV services can provide good opportunities for service providers to enhance their revenue and emerging interactive multimedia markets. Service providers must consider a number of factors to determine the best approach for IPTV deployment. For the IPTV deployment, margins and revenues will be set of challenges, and CAPEX and OPEX should be considered as well. On one hand, the return on investment (ROI) is often unacceptable based on build costs combined with ongoing OPEX. On the other hand, average revenue per user (ARPU) for IPTV in a bundled triple play offering is highly attractive. Providing a complete IPTV ecosystem through a consortium of partners is one of good approaches to minimize risk and reduce the complexity of implementation for a service provider. In this IPTV ecosystem, economic value can be added by combining technology and capabilities from a team of IPTV solutions providers. Therefore, different service providers use portions of the ecosystem in conjunction with other technologies and vendors, where each of the ecosystems partners also works with other vendors. In the meanwhile, the deployment of IPTV service causes big challenges in the construct and management of complex IPTV service infrastructure. It is also recognized that a service provider wants choices and needs flexibility. With IPTV, it is often subjective considerations that drive decisions, not merely economic.
The service provider market is undergoing a major transition resulting from technology evolution and competitive pressures. Service providers need to realize their IPTV infrastructure by weighing the pros and cons of each under consideration of each service provider's unique business objectives.

## 6.6 Cloud computing

**Technical comparison**[164]

In consideration of system migration, there are certain criterions that need to be analyzed to introduce a cloud technology. Selecting SaaS, PaaS or IaaS depends on certain aspects such as SLA, data portability, etc. as follows:

Table 6-6-1. Comparison for cloud technologies

| Migration Criteria | SaaS | PaaS | IaaS |
|---|---|---|---|
| **SLA** | SLA for application's availability, scalability and performance. | SLA for platform availability and performance. | SLA for the availability and |

[163] "Economically Optimized IPTV Triple Play," Zhone White paper, "The Evolving IPTV Service Architecture," Cisco white paper, Ken Kerpez, et, al, "IPTV Service Assurance," IEEE Communication Magazine, Sep. 2006., "IPTV and IMS in Next-generation Networks," Alcatel-Lucent

[164] Adapted from Veeraj Thaploo , "11 Key Criterias for Cloud Migration," AWS Cloud Computing, Tech, Cloud, News & More

| | | | |
|---|---|---|---|
| | | | performance of the server. |
| **Data Portability** | Ability to export all application data that belongs to enterprises. | Data is typically stored in a DB provided by the cloud service provider. | IaaS must provide a way to replicate or migrate the block or file storage. |
| **Long Term Costs** | Compare longer-term recurring costs over time against amortized cost of ownership | Compare costs against internal deployment of the infrastructure over the application server platform. | The cost of an IaaS application should be compared against the cost of deploying that application on enterprise servers. |
| **User Management** | Impact of SaaS application not being able to automatically update the change in the enterprise directory services | Should examine how the user management aligns with their existing directory services and user management process. | Should understand how server administrator and application administrator can be managed. |

**Financial considerations**[165]
It is recognized that the adoption of cloud computing provides significant advantages in aspects of flexibility and convenience. However, the migration to cloud computing would often cause unexpected costs and time consumption. Some operations can turn out to be very costly, particularly if they are not prepared in a timely manner. For example, a one-off transfer of large volumes of data to or from the cloud can be very costly, as can the storage of data in the cloud over very long periods. Such an operation can represent a considerable outlay for a company, which may not be aware of this in the short term. According to the researches of ITU-D on cloud computing, the frequent movement of data between company and cloud can also rack up the costs, particularly in terms of bandwidth consumption where transfer times are lengthy. As things currently stand, then, and aside from long-term storage and the frequent consultation of large volumes of data, it is clear that the other cloud computing services − SaaS, PaaS, NaaS, CaaS – are providing their adherents with very significant gains by comparison with in-house solutions.

According to a recent Merrill Lynch research note, cloud computing is expected to be a "$160-billion addressable market opportunity". As the computing industry shits toward providing PaaS and SaaS for consumers and enterprises to access on demand regardless of time and location, there will be an increase in the number of cloud platforms available. Providers such as Amazon, Google, Microsoft and Sun Microsystems have begun to establish new data centers for hosting cloud computing applications in various locations around the world to provide redundancy and ensure reliability in case of site failures.

- Google Cloud: allows a user to run web applications written using the Python programming language and provides a web-based Administration Console for the user to easily manage his running web applications.
- Microsoft Azure Cloud: provide an integrated development, hosting, and control Cloud computing environment so that software developers can easily create, host, manage, and scale both web and non-web applications through Microsoft data centers.
- Sun Microsystems Cloud: enables the user to run Solaris OS, Java, C, C++, and FORTRAN

165 "Cloud Computing in Africa Situation and Perspectives," ITU-D Apr. 2012.
Bhim Sain Singla, "COMPARISON OF VARIOUS COMPUTING TECHNOLOGIES AND EMERGING CLOUD PLATFORMS," VSRD International Journal of Computer Science & Information Technology, Vol. 2 No. 11 November 2012

based applications.
- Amazon Elastic Compute Cloud: provides a virtual computing environment that enables a user to run Linux-based applications.

## 6.7 Smart Grid

**Technical comparison**[166]
A communications system is the key component of the smart grid infrastructure. With the integration of advanced technologies and applications for achieving a smarter electricity grid infrastructure, a huge amount of data from different applications will be generated for further analysis, control and real-time pricing methods. Different communications technologies supported by two main communications media (i.e., wired and wireless) can be used for data transmission between smart meters and electric utilities. In some instances, wireless communications have some advantages over wired technologies, such as low-cost infrastructure and ease of connection to difficult or unreachable areas. However, the nature of the transmission path may cause the signal to attenuate. On the other hand, wired solutions do not have interference problems and their functions are not dependent on batteries, as wireless solutions often do.

Table 6-7-1. Smart Grid Communications Technologies

| Technology | Spectrum | Data Rate | Coverage Range | Applications | Limitations |
|---|---|---|---|---|---|
| **GSM** | 900-1800 MHz | Up to 14.4 Kbps | 1-10 Km | AMI, Demand Response, HAN | Low data rates |
| **GPRS** | 900 – 1800 MHz | Up to 170 Kbps | 1-10 Km | AMI, Demand Response, HAN | Low data rates |
| **3G** | 1.92 – 1.98 GHz, 2.11-2.17 GHz (licensed) | 384 Kbps – 2 Mbps | 1-10 Km | AMI, Demand Response, HAN | Costly spectrum fees |
| **WiMAX** | 2.5 GHz, 3.5 GHz, 5.8 GHz | Up to 75 Mbps | 10-50 km (LOS), 1-5 km (NLOS) | AMI, Demand Response | Not widespread |
| **PLC** | 1-30 MHz | 2-3 Mbps | 1-3 Km | AMI, Fraud Detection | Harsh, noisy channel environment |
| **ZigBee** | 2.4 GHz, 868-915 MHz | 250 Kbps | 30-50 m | AMI, HAN | Low data rate, short range |

NOTE
- ZigBee is a wireless communications technology that is relatively low in power usage, data rate, complexity, and cost of deployment. It is an ideal technology for smart lightning, energy monitoring, home automation, and automatic meter reading, etc.
- Powerline communication (PLC) is a technique that uses the existing power lines to transmit high-speed (2–3 Mb/s) data signals from one device to the other.

Basically, two types of information infrastructure are needed for information flow in a smart grid system. The first flow is from sensor and electrical appliances to smart meters, the second is between smart meters

[166] Vehbi C. Güngör, et al, "Smart Grid Technologies: Communication Technologies and Standards," IEEE TR on industrial informatics, Vol.7 No.4, Nov. 2011.

and the utility's data centers. The first data flow can be accomplished through power line communication or wireless communications, such as ZigBee, 6LowPAN, Z-wave, and others. For the second information flow, cellular technologies or the Internet can be used. Nevertheless, there are key limiting factors that should be taken into account in the smart metering deployment process, such as time of deployment, operational costs, the availability of the technology and rural/urban or indoor/outdoor environment, etc. The technology choice that fits one environment may not be suitable for the other. In Table 4, some of the smart grid communications technologies along with their advantages and disadvantages are briefly explained.

## 7. Acronyms

| | |
|---|---|
| 3GPP | 3rd Generation Partnership Project |
| 6LowPAN | IPv6 over Low power Wireless Personal Area Network |
| ADSL | Asymmetric digital subscriber line |
| AGW | access gateway |
| AMF | account management function |
| AMI | Advance d Metering Infrastructure |
| ANSI | American National Standards Institute |
| AP | access point |
| API | application programming interface |
| ARPU | Average Revenue Per User |
| ARPU | average revenue per user |
| ASP | Application Service Provider |
| ATM | Asynchronous Transfer Mode |
| BM | burst mode |
| CA | Carrier Aggregation |
| CaaS | Communications as a Service |
| CAF | charging and accounting function |
| CAP | Common alerting protocol |
| CAPEX | Capital expenditure |
| CAS | conditional access system |
| CCF | charging collection function |
| CCIF | Cloud Computing Interoperability Forum |
| CCRA | cloud computing reference architecture |
| CDF | content delivery functions |
| CDMA | Code Division Multiple Access |
| CDR | Call Detail Record |
| CDR | charging data record |
| CM | continuous mode |
| CMTS | Cable Modem Termination Systems |
| CO | Central Office |
| CoMP | Coordinated Multi Point operation |
| CompassS | Compute as a Service |
| CPU | central processing unit |
| CS | Circuit Switched |
| CSA | Cloud Security Alliance |
| CSC | cloud service customers |
| CSP | cloud service provider |
| CTF | charging trigger function |
| DaaS | Desktop as a Service |
| DAB | digital audio broadcast |
| DCIM | Data center infrastructure management |
| DER | distributed energy resource |
| DFT | Discrete Fourier Transform |
| DG | Distributed Generation |
| DHCP | dynamic host configuration protocol |
| DL | Downlink |
| DLNA | Digital Living Network Alliance |
| DMTF | Distributed Management Task Force |
| DOCSIS | Data Over Cable Service Interface Specification |
| DoS | denial of service |

| | |
|---|---|
| DR | Demand Response |
| DR | Disaster Relief |
| DRM | disaster risk management |
| DSaaS | Data Storage as a Service |
| DSLAM | digital subscriber line access multiplexer |
| DSP | Digital Signal Processing |
| DTCP | Digital Transmission Content Protection |
| DVB | Digital Video Broadcasting |
| EAS | emergency alert system |
| EDGE | Enhanced Data rates for GSM Evolution |
| EFM | Ethernet in the First Mile |
| EISA | Energy Independence and Security Act |
| EMS | Energy Management System |
| EPG | Electronic program guides |
| EPON | Ethernet passive optical networks |
| EPS | Evolved Packet System |
| ET | Emergency Telecommunication |
| ETS | Emergency Telecommunication Service |
| E-UTRAN | Evolved Universal Terrestrial Radio Access Network |
| EW | Early Warning |
| FAP | Femtocell Access Points |
| FDD | frequency-division duplexing |
| FE | functional entity |
| FG-Cloud | Focus Group on Cloud Computing |
| FGW | Femto Gateway |
| FMC | fixed and mobile convergence |
| FMS | Femto Management System |
| FTTB | Fiber to the Building |
| FTTB | Fiber to the Business |
| FTTC | Fiber to the Curb |
| FTTD | Fiber to the Desktop |
| FTTE | fiber-to-the-telecom-enclosure |
| FTTH | Fiber to the Home |
| FTTK | Fiber to the kerb |
| FTTLA | Fiber to the Last Amplifier |
| FTTN | Fiber to the Neighbourhood |
| FTTP | Fiber to the Premise, or Pole |
| FTTX | Fiber to the X |
| FTTZ | fiber-to-the-zone |
| GDP | Gross domestic product |
| GFoG | Radio frequency over glass |
| GHG | greenhouse gas |
| GIS | Geographic Information Systems |
| GPON | Gigabit-capable passive optical networks |
| GPRS | General packet radio service |
| GSM | Global System for Mobile Communications |
| GSMA | Groupe Speciale Mobile Association |
| HAN | Home Area Network |
| H-ANI | home network Application Network Interface |
| HDSL | High-bit-rate Digital Subscriber Line |
| HFC | hybrid fibre/copper |
| HSPA | High Speed Packet Access |
| H-TNI | home network terminal network interface |
| IaaS | Infrastructure as a Service |
| ICT | Informaiton Communication Technolgy |
| IdM | identity management |

| | |
|---|---|
| IEC | International Electrotechnical Commission |
| IEEE | Institute of Electrical and Electronics Engineers |
| IEPREP | Internet Emergency Preparedness |
| IESG | Internet Engineering Steering Group |
| IETF | Internet Engineering Task Force |
| IMS | IP Multimedia Subsystem |
| IMT | International Mobile Telecommunication |
| IP | Internet Protocol |
| IPR | Intellectual Property Right |
| IPTV | Internet Protocol Television |
| ISDN | Integrated Services for Digital Network |
| ISDR | International Strategy for Disaster Reduction |
| ISIM | IMS subscriber identity module |
| ISO | International Organization for Standardization |
| ISP | Internet Service Provider |
| IT | information technology |
| ITF | IPTV terminal functions |
| ITS | intelligent transport systems |
| ITU | International Telecommunication Union |
| ITU-D | ITU Telecommunication Development Sector |
| ITU-R | International Telecommunication Union Radiocommunication Sector |
| ITU-T | International Telecommunication Union Telecommunication Standardization Sector |
| JPEG | Joint Photographic Experts Group |
| LAN | Local Area Network |
| LROAN | Long-Reach Optical Access Network |
| LSI | large scale integration |
| LTE | Long-Term Evolution |
| MAC | Media Access Control |
| MAN | Metropolitan Area Network |
| MBMS | Multimedia Broadcast Multicast Service |
| MBSFN | Multicast-Broadcast Single Frequency Network |
| MDU | Multi-Dwelling Unit |
| MEG | micro energy grid |
| MIMO | Multiple-Input and Multiple-output |
| MPEG | Moving Picture Experts Group |
| MSO | Multiple System Operators |
| NaaS | Network as a Service |
| NACF | network attachment control function |
| NAT | network address translation |
| NE | network element |
| NGHN | Next generation home network |
| NGN | Next Generation Network |
| NIST | National Institute of Standards and Technology |
| NMS | network management system |
| NNI | Network to Network Interface |
| NRR | Network Resilience and Recovery |
| NTE | Network Termination Equipment |
| OAMP | Operations Administration Maintenance and Provisioning |
| OCC | Open Cloud Consortium |
| OCF | online charging function |
| ODN | optical distribution network |
| OECD | Organisation for Economic Co-operation and Development |
| OFDMA | Orthogonal Frequency-Division Multiple Access |
| OGF | Open Grid Forum |
| OLT | Optical Line Terminal |
| ONU | Optical Network Unit |

| | |
|---|---|
| OPEX | Operational Expenditure |
| OS | operating system |
| PaaS | Platform as a Service |
| PAM | PSTN Access for Mobile users |
| PAN | Personal Area Network |
| PAPR | Peak-to-Average Power Ratio |
| PC | personal computer |
| PDA | personal digital assistant |
| PEV | plug-in electric vehicles |
| PLC | Power Line Communication |
| PLMN | public land mobile network |
| PON | Passive Optical Network |
| POTS | plain old telephone service |
| PPP | public-private partnership |
| PS | Packet Switched |
| PSTN | public switched telephone network |
| PUE | Power Usage Effectiveness |
| QoE | Quality of Experience |
| QoS | Quality of Service |
| RACF | resource and admission control functions |
| RES | renewable energy source |
| RF | Radio Frequency |
| RF | rating function |
| RF | Rating Function |
| RIT | Radio Interface Technologies |
| RN | Relay Nodes |
| ROI | return on investment |
| RSS | Rich Site Summary |
| SaaS | Software as a Service |
| SAC | service access code |
| SAME | specific area message encoding |
| SCADA | supervisory control and data acquisition |
| SC-FDMA | Single Carrier Frequency Division Multiple Access |
| SCP | Service and content protection |
| SDH | Synchronous Digital Hierarchy |
| SDK | software development kit |
| SDO | Standards Development Organization |
| SeGW | Security Gateway |
| SG | Study Group |
| SGCC | Study Group on Cloud Computing |
| SIP | Session Initiation Protocol |
| SLA | Service Level Agreement |
| SNIA | Storage Networking Industry Association |
| SOA | Service-Oriented Architecture |
| SONET | Synchronous Optical Networking |
| SSC | Sustainable Smart City |
| SSDM | Smart Sustainable Development Model |
| STB | Set Top Box |
| TDD | Time-division duplexing |
| TDM | Time Division Multiple Access |
| TDR | Telecommunication Disaster Relief |
| TR | Technical Report |
| TWG | Telecom Working Group |
| TX | Transmit |
| UA | Universal access |
| UAS | universal access and service |

| | |
|---|---|
| UE | User Equipment |
| UI | User Interface |
| UICC | universal integrated circuit card |
| UL | Uplink |
| UMA | unlicensed mobile access |
| UMTS | Universal Mobile Telecommunication System |
| UN | United Nations |
| UNI | User Network Interface |
| US | universal service |
| USF | Universal Service Fund |
| UWB | Ultra Wideband |
| VDSL | Very-high-bit-rate digital subscriber line |
| VoD | Video on Demand |
| VoIP | voice over IP |
| VPN | Virtual Private Network |
| WAN | Wide Area Network |
| W-CDMA | Wideband Code Division Multiple Access |
| WDM | Wave Division Multiplexing |
| WG | Working Group |
| WiMAX | Worldwide Interoperability for Microwave Access |
| WLAN | Wireless Local Area Network |
| WP | Working Party |
| XDSL | X Digital Subscriber Line |

## 8. Reference Standards/Publications

- A List of  ITU Publications and Standards cross-referenced in the document is available on-line (Link)