CHAPTER 4
ITU-T FUTURE NETWORKS

4.1 Introduction

Y.3001 Recom. of International Telecommunications Union-Telecom design goals and objectives of future networks (FNs) give differences between the network of the future and current network. The design goals and objectives are illustrated by figure 4.1

![Figure 4.1: Twelve design goals & four objectives of future networks](image)

These design goals are reliability & security, Identification, optimization, mobility, NW management, economic incentives, service utilization, energy consumption, data access, virtualization of resources and functional flexibility.

- **Security & Reliability**: The users of Future NWs must be safe and their privacy should be maintained at any cost. Future Network should be safe,
resilient, reliable, evolutionary in nature & fault tolerant to all changing conditions. It should be reliable and integral with other networks and must withstand critical services like emergency telecommunication, e-security, e-health, smart grids and intelligent traffic management (example: space traffic, marine traffic, air traffic, rail traffic & road traffic) (Y.2205 of ITU-T, May 2014). Resilient makes future network able to ascertain to users that it will give minimum level of service even during various challenging and faulty conditions. The characteristics of resilient is challenge tolerance & trustworthiness. Trust is gained by network of the future where it assures the users that they will receive secure and dependable performance by the system. Many challenging situations such as challenges by environment (mainly in wireless networks), legitimate but unusual traffic, bad configurations, cyber related or real world attacks, man made or natural disasters & natural faults (example: hardware aging) may threaten systems' trustworthiness. There is a discipline called challenge tolerance which takes care about the engineering & design of future networks so that it could withstand all such types of challenges to give continued service. Traffic tolerance, disruption tolerance & survivability are the sub-disciplines of challenge tolerance. These sub-disciplines deal with these challenging situations which makes the systems of future networks capable of fulfilling the mission within acceptable timeframe.

- **Identification:** A new structure of identification supporting scalability, access to data & mobility should be provided by future networks. The main design aim of the network of the future should be such that the communication objects should be provides scalable and efficient identification. Instead of identifying hosts by IP addresses as it is done in present NWs, Future NWs should use host locators (attachment points) for identification.

- **Optimization:** Based on the demand of users and requirement of services, capacity of the NW equipments should be optimized so that enough performance could be provided by Future Network while considering and taking in to account the NWs' equipments physical limitations.

- The networks are supposed to be large scale, high speed and heterogeneous, therefore, mobility and movement of nodes should be facilitated seamlessly by
Future Networks & all types of mobile services irrespective of capability of node mobility should be provided.

- **Network Management:** Future Networks be capable of handling & maintaining increased number of entities & services & must be capable of operating efficiently in these circumstances. Particularly, Future Networks should have capability of processing large amount of information & data related to management tasks. These information & date should be transformed in an effective and efficient manner into knowledge & information relevant to the operator of the network.

- **Economic Incentives:** Future networks should provide a suitable economic incentives to participating parties in ecosystem of Communication & Information/telecommunications technologies systems such as IPR holders, governments, service providers & users to solve tussles among them.

- **Service Universalization:** Through principles of open network & through reduction of its life cycle costs, Future Networks should provide and accelerate facilities in various areas, for example, developing countries or developed countries, countryside or towns. To reduce NWs' lifecycle costs particularly costs of management tasks, operation, deployment & development, openness through simple design & global standards should be supported by Future Networks. These things reduce digital divide.

- **Energy Consumption:** For the satisfaction of demands of customers & improvement in energy efficiency with least traffic, Future Networks should use NW level technologies, equipment level technologies & device level technologies. For saving the energy of network, these various levels of technologies should cooperate with each other. To operate network properly, energy saving is an important factor because excessive consumption of energy will dissipate large amount of heat from the equipment which may damage it thereby preventing the offerings of applications and services.

- **Data Access:** Huge amount of video, audio, text & multimedia data are created and generated by different applications using Internet which are stored and processed, stored Y distributed across the networks. These large amounts
of data should be handled efficiently & optimally by proper design & implementation of Future Networks. Irrespective of location of data, Future Network should have technology to facilitate prompt and easy retrieval of these data & information.

- **Virtualization of Resource:** Resources across the network are partitioned physically called virtual resources. Out of these resources, there may be concurrent sharing of any virtual resource. These individual virtual resources should be isolated & shared by Future Networks. Thus, Future Networks should have the capability to abstract virtual resource from its corresponding physical characteristics.

- **Functional Flexibility:** Demands of users should be fulfilled by new services of future Networks which should be flexible enough to derive services to fulfil these demands. Terminal devices, sensors etc constitute wide variety & large number of communication objects which must be supported by Future Networks. Based on the particular demands of the different NW services, Future Networks should be capable of modifying the NW functions dynamically.

- **Service Diversity:** Accommodation of different variety of traffic and wide range of services should be supported by Future Networks. Terminal devices & sensor like large number of communication objects should be supported by Future Networks.

The following objectives reflecting the emerging requirements should be fulfilled by Future Networks:

- **Social & Economic Awareness:** Economic and social issues should be considered while designing Future Networks. This will help in reducing hindrances in the path of different types of actors entering in to the NW economic system. A sustainable & deployable Future networks should be designed so that costs of their lifecycles could be reduced and entry of actors could be easy. These things will help in allowing suitable returns and satisfaction for every actor involved. This will also help in permitting appropriate competition among actors and universalization of services.
• **Environmental Awareness:** The design of Future Networks' architecture should be environmentally friendly & the resulting implementation & operation should minimize any bad impact on environment. For example, Future Network should reduce greenhouse gas emissions & consume less energy & materials. Impact of environment due to other sectors should also be taken care while designing Future Networks.

• **Data Awareness:** In distributed environment, for handling data of huge amounts, the architecture of Future Networks should be optimized. Irrespective of the location of data, users of the Future Networks should be enabled to access the required data of any type accurately, quickly, easily, & safely.

• **Service Awareness:** Appropriate services in required range and number needed by users and applications should be provided by Future Networks. Since there will be explosion of range and number of services in near future, these services should be accommodated by Future Networks without exorbitant increase in operational & deployment costs.

**Design Goals & Technology Needed to Achieve It**

Following technologies are needed to achieve the design goals of Networks of Future:

- Virtualization of resources & networks
- Networking with characteristics of distributed mobility
- Optimizing the NW
- Management of Network In-system
- Networks' energy management
- Networks having orientation towards content/data

A wide variety of architectures of networks, services and applications should be provided by Future Networks. Virtualization process partitions the entire physical networks into smaller networks which are isolated logically and thus creates a large number of heterogeneous networks whose physical resources can be shared and
allowing them to coexist side by side without troubling the others. Virtualization also aggregates and combines may physical resources into a single resource in logical appearance. Elements of logically partitioned networks can be programmed and thus newer technologies can be imported dynamically & configured into equipments such as routers & switches which are virtualized. With the help of virtualization, many globally spread & individually managed isolated networks can be federated & combined into a single NW thus allowing services to move from one element to another. Which results in the location and access of remote elements and services by the users.

Networking with distributed mobile functions acts as fault tolerant and bottleneck issues & failure at single point can be isolated.

The design of future networks should be so effective that it should provide users with optimized capacities & capabilities of network resources.

In-system NW management is a network management which controls complexity of management with decentralized approach whose fundamental concepts are autonomicity, autonomy, self organization & decentralization.

Future Network should use the proper network level, equipment level & device level technologies to minimize energy consumption.
4.2 ITU-T Future Network Framework of Network Virtualization

Since realization of heterogeneous network architectures of multiple physical networks require huge costs on installation, operation and maintenance, therefore, a common physical network is required for future network to realize diverse services and heterogeneous network architectures. Since future and emerging network services require high-speed, large volume, low latency network connectivity for voice, video, and data base communications, it is necessary to ensure low power consumption by future networks. Future networks should also be more flexible and more reconfigurable so as to adapt to the changing requirements for future network services and applications.

To make diverse services flourish, the FNs should provide easy methods for experimenting and/or small scale deployment without causing unexpected effects for other networks that is why it is often done by building completely separate networks. It will be an ideal environment to design, develop, and evaluate new services for developers, providers and the users of emerging technologies if experimental networks and/or test beds could be built on real networks that share common physical networks and could still provide isolated network environment.

These types of isolated and flexible networks are realized using network virtualization technology which supports a broad range of network architectures, services, and users that do not interfere with others. Thus, network virtualization is considered as a key technology for realizing future networks because it enables the easy establishment of experimental networks and accelerates research and development on future network technologies (ITU-T recommendation Y. 3011, 2012).

4.2.1 Network Virtualization Overview

A method that allows multiple virtual networks to coexist in a single physical network is called network virtualization. These multiple virtual networks are called logically isolated network partitions (LINPs). Physical resources are partitioned and abstracted as virtual resources. These virtual resources are interconnected to create a logically isolated network partitions (LINP) (Chowdhury, N.M. and Boutaba, R., 2010), (GENI, 2006) (Nakao, A., 2010). These virtual resources can be created on physical resources such as hosts, switches, and routers. Either virtual resources are
allocated to each logically isolated network partition or multiple virtual resources are aggregated into a single virtual source.

In an LINP network, virtual resources are separated from others and its capability can be reconfigured dynamically. It is a logical partition of the physical network having the same capability as that of physical network from which it is derived. It can also increase its capability by aggregating the multiple virtual resources. A user views the LINP as a network without network virtualization. A virtual resource is an abstraction of a physical or logical resource and its partition. It has the same mechanism as the physical or logical resource from which it is abstracted. Also, all the existing mechanism and tools for the physical or the logical resource from which it is abstracted can be inherited. In addition, a virtual resource has several interfaces to access and manage the virtual resources. Data plane interfaces, control plane interfaces, and management plane interfaces are typically included in these interfaces. (Vernesan, O. and Friess, P., 2011).

Conceptual architecture of network virtualization is represented in Figure 4.2 (ITU-T recommendation Y. 3011, 2012). This consists of LINPs over physical resources supporting network virtualization. Multiple virtual resources can share a single physical resource where each LINP consists of multiple virtual resources. An individual LINP manages each individual LINP. Physical resources in a network(s) are virtualized forming a virtual resource pool (Figure 4.2). Virtual resource manager (VRM) manages these virtual resources. The virtual resource manager interacts with the physical network manager (PNM) and performs control and management of virtual resources. Once virtual resources construct an LINP, an LINP manager is allocated to the LINP where the LINP manager performs a management function.
The concept of LINP is represented in Figure 4.3 which consists of multiple coexisting LINPs over network resources supporting network virtualization. User requirements decide provision of each LINP. Administration policy of VRM handles the requirement of LINPs. An LINP manager controls and manages each LINP. The VRM creates an LINP manager and allocates appropriate authorities to control each LINP.
Figure 4.3: Conceptual Architecture of Network Virtualization.

An LINP has various characteristics as detailed below (Vermesan, O. and Friess, P., 2011), (Nakao, A., 2010):

- **Authentication**, Authorization, and Accounting: Usage of virtual resources which created an LINP must be authenticated and authorized to achieve safe and secure operations of LINPs. It prevents the abuse of the virtual resources and malicious attacks on them. To examine and monitor and to optimize the usage of virtual resources, it is necessary to account for the allocated virtual resources in physical networks.

- **Programmability**: LINPs' virtual resources can be programmed to develop, deploy and experiment with new communication protocols for innovative data dissemination and to facilitate efficient data processing to be enabled within the LINP.
• **Flexibility (Elasticity):** In order to maximize the usage of physical resources, LINPs' virtual resources are flexibly allocated, reclaimed, and released on demand. Flexibility also allows instantaneous and bursty usage as well as continuous usage of physical users.

• **Isolation:** All the virtual resources of one LINP are isolated from the other LINPs' virtual resources so that LINPs could not interfere with one another in terms of performance, security and namespace or any single LINP could disrupt other LINPs or physical networks. Also isolation prevents leak of data across LINPs.

• **Abstraction:** A virtual resource can be abstracted directly from its physical resource and need not correspond directly from its physical resource so that other systems, applications or users access the capabilities of the virtual resource by using abstracted interfaces. These interfaces provide an efficient control of the virtual resource and guarantee compatibility for accessing the virtual resource. Interfaces can also be extended in order to provide increased capabilities. Through well defined and extensible interfaces, the virtual resources can be manipulated. These extensible interfaces can also be allocated to create, modify, reclaim, and release LINPs.

• **Partitioning:** Each LINP contains a set of resources which are independently manageable partition of physical resources. On a physical network, multiple LINP can coexist.

In a nutshell, Utilization of physical resources can be improved by network virtualization by allowing multiple virtual resources to coexist in a physical resource. The abstraction and programmability also properly provides standard interfaces for managing and modifying the LINPs. It also gives a helping hand to support seamless modification and migration of the network so that it could provide services whose functions are designed to be appropriate to the needs of applications and users.
4.2.2 Problem spaces

Network virtualization can be used to mitigate the problems of current networks as discussed below:

• **Evolvability:** The disadvantage of building a separate physical test-bed is that the new technologies and services that have been successfully evaluated in the test-bed may not operate well in the real networks. Another disadvantage is the possibility of losing legacy support or backward compatibility. Network virtualization permits the network providers to integrate legacy support by allocating the existing networks to LINPs where the LINPs will ensure that the existing services and technologies can remain unchanged.

• **Flexibility in Provisioning:** Quick reconfiguration of LINPs is provided by network virtualization to enhance flexibility to environmental changes such as sudden traffic demand changes and network failures by dynamically changing their configurations. Network virtualization also allows adding additional logical resources to a virtual resource so that it could provide increased capability at lower cost than by adding physical resources.

• **Simplified access to resources:** Heterogeneity of multiple heterogeneous physical resources could cause difficulty in accessing and managing the networks because of different types of access interfaces. Interoperability among various heterogeneous network resources is an important factor for future networks. Network virtualization allows the other systems, applications, or users to access the capabilities of resources by using abstracted interfaces (Vermesan O., and Friess P., 2011). These interfaces allow efficient access and control of virtual resources.

• **Coexistence of Multiple Networks:** Conventional technology such as virtual private network (VPN) suffer from disadvantages in scalability, performance, and throughput so adding VPN mechanisms to existing protocols brings additional complexity and high data-processing costs (Burger t., 2006). It also suffers from considerable performance issues such as home agents and mobile nodes (IETF RFC 4093, 2005), (IETF RFC 5265, 2008). Another conventional technology, virtual local area network (VLAN) suffers from
scalability problems due to size of address space. By interconnecting virtual resources, network virtualization can provide LINPs where the interconnections may be realized by various mechanisms not limited to conventional mechanisms (such as VPN and VLAN) according to user and service requirements. Network virtualization can also provide secure isolation among LINPs from various points of view which includes security, performance or management, and support diversity of application, service management, network control, and architectures.

4.2.3 Design goals

Design goals of realizing network virtualization cover various aspects such as capabilities, characteristics and some challenging issues which are investigated below:

- **Wireless:** Wireless links should be virtualized. If two LINPs coexist on the same hardware for user, communication activities from one LINP should not affect any reception behaviour on the other LINP. Coherence (when a transmitter of one LINP is active, all of the corresponding receivers and potential sources of interference should be simultaneously active on their appropriate channels of operation), and isolation (when a node belonging to one LINP is receiving some signal pertinent to the LINP, no transmitter of a different LINP within the communication range of the receiver should be active in the same or partially over-lapping channel) characteristics of the wireless links should be maintained (Mishra, A. et al., 2006). Therefore, scheduling methods for transmission activities across different LINPs should be maintained (Smith, G. et al., 2007).

- **Mobility:** Mobility is the ability of movement of virtual resources, including users and services which are composed of, for example, computing resources, system images, and applications across LINPs. Network virtualization should support mobility in order to fulfill the requirements of LINPs.

- **Management:** Network virtualization should provide an integrated management system that can access both the information of physical resources and virtual resources to manage the network operations such as monitoring,
fault detection, topology awareness, reconfiguration, resource discovery/allocation/scheduling, and customized control.

- **Programmability:** Users can customize protocols for forwarding or routing functions by equipping LINPs with programmable control plane and data plane. Programmability can support flexibility in the control plane for easy adaptation of new control schemes on LINPs and also in data plane to enable different kinds of data processing. Therefore, in order to provide flexibility and evolvability of networks using new control schemes and new data processing capabilities, network virtualization should support both control and data plane programmability.

- **Performance:** Network virtualization adds additional virtualization layer which adds overhead and degrades system performance including higher CPU utilization and lower bandwidth, therefore, the performance of the LINPs may not be as good as that of non-virtualized network. The performance degradation of virtualized networks, therefore, should be minimized.

- **Topology awareness and quick reconfigurability:** During the construction of LINPs, network virtualization should support topology awareness so that the virtual resources can effectively interact with each other. During the operation, each LINC needs to adjust its capability according to the changes of requirements and, therefore, the reconfiguration should be quickly done in order to minimize service disruption. Thus, network virtualization should offer methods for easy and rapid creation of LINPs and should dynamically reconfigure them.

- **Network abstraction:** Hiding the underlying characteristics of network resources and establishing simplified interfaces for accessing the network resources (called network abstraction) allows the selective exposure of key network functionalities in networks by defining the abstraction level. It opens a new possibility to provide higher level interfaces thereby increasing the accessibility.
• **Isolation**: LINPs can cause instability due to interference with each other. Network virtualization can mitigate these problems by providing secure isolation, such as performance and security, among LINPs.

### 4.2.4 Applicability

The key characteristics and the design goals of network virtualization will be catalytic factors for achieving the objectives and design goals of the future networks. The factors such as isolation of multiple LINPs, abstraction of network resources, flexibility in configuring and providing LINPs, and support of mobility and wireless virtualization can contribute in realizing the objectives and design goals of the FNs. Network virtualization also has several disadvantages as mentioned below:

- Performance degradation of LINPs,
- Scalability issues for the number of possible LINPs in a shared physical network, and
- Possibility of crashing whole LINPs due to the failure or security problems on LINP management systems.

Thus, both advantages and disadvantages should be carefully considered from the initial stage before developing and deploying network virtualization to current networks.

### 4.2.5 Environmental considerations

By changing the overall architecture of networks through network virtualization, resource consumption and energy consumption is changed. Network virtualization also enables operators to develop multiple LINPs on a single physical network which reduces the necessary physical resources for constructing networks. For example, reduction in use of optical fibre or copper cable generally reduces energy consumption. Hardware utilization is improved by allowing more than one service to operate on the same piece of physical resource by network virtualization. This lowers the energy consumption because a single machine under high load generally consumes less energy than several lightly-loaded machines. Also, resource consolidation can be achieved by network virtualization which regroups underutilized devices which further reduces the energy consumption. The drawback of the network
virtualization is that the structure of each node such as routers and switches become more complicated, which may cause increase in energy consumption.

4.2.6 Security considerations

Since virtual resources of LINPs are made available to the users, therefore, various securities need to be provided to the LINPs. Security and privacy problems related to public cloud computing services, as investigated by [b-Jansen] can be applied to the network virtualization. In order to mitigate potential security problems, the security and privacy issues such as security and privacy requirements of users, service providers using LINPs, and LINP providers should be considered. Also, the security and privacy of data and applications that are implemented and deployed in LINPs should be regularly kept under monitoring.
4.3. Energy Saving Framework for Future Networks

Energy saving framework for future networks is described in (Recommendation ITU-T Y.3021, 2012) which describes the need for energy saving within networks and reviews technologies for potential energy savings. The recommendation describes energy saving necessities, reviews potential technologies, identifies multiple viewpoints, major functions and their cyclic interactions. It also introduces technologies and analyzes any possible impact caused by it, and also itemizes high level requirements.

4.3.1 Introduction

Environmental awareness is one of the basic features of future networks development which is realized via energy saving technologies. Energy saving increases benefits to the company or users, such as reduced costs of energy and temperature management for stability of machine operation. Because of widespread implementation of network equipments and the greater energy consumption required by these equipments, and also the social aspect of supporting the reduction of greenhouse gas (GHG) emissions increases the importance of these issues. To reduce the negative impact of environment, information and communication technology (ICT) is categorized into:

- "Green by ICT", and
- "Green ICT"

To reduce the environmental impact of the non-ICT sectors by using ICTs is referred to as "Green by ICT" while to reduce the environmental impact of the ICT itself, for example, electric power consumption reduction of personal computers, routers and servers. Therefore, Future networks contribution in reduction of environmental impact can be categorized as:

- "Green by Future Networks", and
- "Green Future Networks"

Design of Future NWs shall be such that it shall decrease other sectors’ environment impact. For example, design of network architecture for eclectic power distribution of
smart grids, or ubiquitous sensor networks that monitor environmental changes of the earth are few examples of "Green by Future Networks".

Future networks must have minimum impact on the environment. "Green by Future Networks" reduces the environmental impact of other sectors. In this process, the future networks increase the volume of traffic flowing into networks and thus increase the energy consumption of the networks which then increase the environmental impact. "Green Future Networks", which means energy saving within the networks themselves, reduces the energy consumption of network facilities such as desktops, servers, routers, switches, etc.

In life-cycle management stages such as, 'production (preparation of raw materials and components for the target), manufacturing, use, and disposal/recycling', attention must be paid to reduce the energy consumption. At each stage, a variety of technologies at different levels such as device-level (electronic devices as large scale integration (LSI) and memory), equipment-level (one piece of equipment (a set of devices) such as router or switch), and network-level (equipments within the whole network (e.g., a routing protocol applied to multiple routers)) should be for energy saving within the networks.

4.3.2 Energy-Saving Technologies

Various potential technologies can be categorized as follows:

- **Device-level technology**
  - **LSI microfabrication**: The thinner the LSI process becomes, the smaller the size of the LSI, therefore, microfabrication enables reduced driving voltage. Since the power consumption is proportional to the square of the driving voltage, therefore, microfabrication reduces energy consumption.
  
  - **Multi-core central processing unit (CPU)**: Using multiple CPU cores in a single processor package can generally save more energy than using a single high-speed CPU because of the hardware characteristics of the electronic devices. Also, a multi-core CPU can run together with dynamic control technologies such as clock gating and sleep mode.
Since clock gating and sleep mode controls energy, minimum required number of CPUs can operate at minimum clock rate thereby saving the energy.

- **Clock gating**: Clock gating technology stops supplying clock to LSIs and circuits when there are no necessary talks, thus saving the energy.

- **Power aware virtual memory**: This technology optimizes the energy consumption in memories such as buffer memory and cache memory in a network node by controlling an active piece of memory depending on actual demand and use (Huang H., et al., 2003).

- Advanced **power amplifier (PA)**: Using high-efficiency power amplifier, which uses digital pre-distortion (DPD) and high-voltage heterojunction bipolar transistor (HVHBT) technologies, used in base stations in wireless networks can reduce power consumption (ATIS, 2010).

- **Equipment-level technology**

  - **Optical network node**: Optical switching does not need optical to electric and electric to optical translation which consumes a large amount of energy in a network node. This can drastically improve network energy efficiency since an optical network node with speeds of Tbps or more has a very large capacity compared with the electronic network node.

  - **Sleep mode control**: Equipments such as routers and switches in wired networks and radio base stations and mobile devices in wireless networks use "sleep mode" technology which shuts down (turns off) the equipments whenever there is no traffic thus saving the energy. Energy efficient Ethernet protocol developed (IEEE P802.3az) is an example of sleep mode control. The L2 power saving mode (e.g., low power mode) combined with existing ADSL2 plus technologies is another example of sleep mode control.
o **Adaptive link rate (ALR) and dynamic voltage scaling (DVS):** For network equipment ALR and DVS are the energy saving operation modes in which ALR controls the link speed (i.e., bit rate) of the interface according to the amount of traffic to be processed and DVS controls the driving voltage of the CPU, hard disk, network interface card (NIC), and so on, according to the amount of traffic to be processed.

o **Thermal design:** Energy saving can be achieved by the improvement of thermal design of the nodes in a network because the cooling system consumes a considerable amount of energy.

o **Cache server:** A Web content with a high hit rate, i.e., multiple users consuming a single content or a single user consuming a content multiple times are cached to reduce bandwidth and energy consumption.

o **Filtering:** Inessential or invalid data to be transmitted like extra keep-alive messages/duplicate user-messages are blocked by this technology. Intrusion detection or prevention systems which prevent/block detected intrusions such as distributed denial-of-service (DDoS) attack by monitoring network traffic for malicious activity is an example of this technology.

o **Sorry server:** If the requested service is not available due to some reasons such as temporal traffic congestion, this technology informs the user about unavailability of the message, thus reducing the maximum traffic and therefore saves energy.

o **Shaping:** This technology controls the output rate of packets lower than the maximum data rate and thus can save the energy of other subsequent nodes.

o **Compact based transceiver stations (BTSs):** Compact BTSs, unlike the ground-based BTSs, don’t need cooling & ground shelters equipments. Therefore, compact BTSs consume less energy, are cheaper, and incur less installation costs.
- **Smart antenna technologies**: Due to the relay nodes, data can be delivered through multiple wireless links, which means each link has independent fading channels. Therefore, diversity gains and spectral efficiency can be improved which reduces the time to transmit a fixed amount of data thereby saving energy.

- **Relay stations**

*Network-level technology*

- **Circuit switching and burst switching**: Less energy is consumed in circuit switching than packet switching because packet switching requires energy consuming memory devices such as SRAM and CAM and accounts for 37% of all power consumption of routers (Baliga, J. et al., 2007). Circuit switching, which is expected to increase drastically in future, is especially efficient for continuous traffic such as video streaming. Burst switching also saves energy consumption in core routers because packets are aggregated into data bursts at edge routers and computing each packet header at edge router reduces the operations at core routers for computing each packet header (Kim Y., et al. 2010).

- **Energy consumption-based routing/traffic engineering**: This is a routing/traffic engineering technology which may include some traffic processing such as traffic aggregation, multiple path routing, and network coding for the purpose of controlling the traffic route to minimize network-wide energy consumption.

- **Lightweight protocol**: This technology uses a protocol in conjunction with protocols with other layers to optimize its use to make the total protocol processing in a network lightweight. One approach is to transfer the data traffic by lower layers which may be applicable to a dedicated area such as a core network. Example of this approach includes multi-protocol label switching (MPLS), performed under the IP layer. The second approach is to make the protocol or its use simple example of which includes convergence by extending the IP capability
form an access network to its backhaul to utilize full IP networking as a common platform (ATIS, 2010). This approach uses a modified TCP that improves the retransmission algorithm, & CAPWAP protocol that reduces the signalling overhead for the wireless local area network (WLAN) (IETF CAPWAP Working Group). Thus, unnecessary function of the network nodes can be reduced by this technology which in turn saves energy.

- **Transmission scheduling:** Buffers at the network nodes are reduced by this technology by minimizing output waiting time at each node end, thus operates with fewer buffers and saves energy.

- **Content delivery networks (CDN):** It is an optimized network especially designed for contents delivery which can save energy because it can access a server that is nearer than the original one. Thus it can save energy by saving resources in terms of bandwidth and distance (Klein T.).

- **Traffic peak shifting:** This technology shifts as much transmission of the traffic as possible onto time axis by distributing popular contents to major cache servers in advance, during off-peak hours, thereby reducing the total power consumption.

- **Small-cell design:** A small cell needs less power to transmit the data traffic compared to a macro cell because the power loss over a wireless channel is proportional to the propagation distance. Thus by designing smaller cells (microcells, picocells, femtocells) to be placed where mobile traffic is high such as city down towns, shopping malls, airports, campuses and large offices etc. Can save energy. But if we consider static power, circuit power, site cooling power as well as transmitting power, small cell-design is not always energy efficient (Chen Y. et al., 2010). Also, small-cell design technologies are typically implemented in the Compact BTSs with Macro BTSs, establishing the overlay cellular networks.
• **Energy consumption-aware network planning:** Network wide design and planning applied to both wired and wireless networks are covered in this technology. Apart from network performance and reliability attention is also given on improvement of energy efficiency and the reduction of the environmental impact. For this purpose, apart from traditional information such as network outage reports (e.g., number of losses, duration of outage), information on energy consumption report should also be collected.

There are two types of energy consumption-aware network planning: static and dynamic. The static part is effective in network design (pre-operation) phase while the dynamic part is effective in operation phase. Energy consumption-aware network planning can result in significant energy saving (Chabarek J. et al., 2008). Cell zooming is one example of dynamic network planning in wireless networks. Cell zooming is required in balancing the load while transferring load from heavy-loaded cells to lightly-loaded cells (Zhisheng, N. et al., 2010).

• **4.3.3 Consideration for Energy Saving:** Here, considerations are made regarding directions to be taken so as to achieve energy saving from the technologies listed in the previous clauses.

  • **Target areas of Recommendation ITU-T Y.3021:**

    - "Green Future Networks" or "Green by Future Networks"

    - Stages in life cycle focuses on the use of stage which includes the pre-operation and operation phases. The pre-operation phase treats the static issue while operation phase treats the dynamic issue. How to minimize the amount of network resources prepared for the given traffic demand in the network design comes under static issue while dynamic issue covers how a smaller amount of network resources could be used according to the traffic at a given moment in the network operation.
- Level of technologies recommendation considers three levels of technologies: device, equipment and network levels. Each technology cooperates with others at different levels and its objective is to find an all-encompassing solution which incorporates each level of the technology.

- Types of methods for energy saving recommendation focuses on technical methods. Regulation by law which assigns individual usage time of networks to each predefined user group is a typical example of non technical methods. This recommendation focuses on technical methods because this recommendation is a technical one.

  **Approach to Energy Saving:**

  1. reduction of required network capacity can be archived by reducing the volume of traffic at peak time which reduces the maximum capacity. Reduction of the required network traffic approach is based on the amount of traffic as shown in Figure 8.2. Reduction of traffic results in the reduction of network resources and capacity, thus reducing the energy consumption.

![Figure 4.4: Energy Consumption V/S Network Capacity](image)

**Figure 4.4: Energy Consumption V/S Network Capacity**
2. Improvement in network energy efficiency can be achieved by controlling devices and/or equipment operations according to traffic dynamics and forwarding traffic with less power. This approach is shown in figure 8.2 and example of controlling device approach is "sleep mode" control which is a static control. An example of forwarding traffic with less power is an optical network with less electrical interventions.

- **Controlling Device and/or Equipment Operation According to Traffic Dynamics:** Technologies which focuses on traffic dynamic like dynamic voltage scaling (DVS) & sleep mode control can save more energy when networks have many nodes in sleep mode or scaled down in terms of voltage. By putting a device to "sleep mode", i.e., device not in use, energy is saved. Similarly, DVS reduces the traffic forwarding capacity of devices such as CPU, line cards, and network interface cards (NIC) when the traffic volume is low.

- **Forwarding Traffic with less Power:** Device level technologies such as LSI microfabrication and an optical network node requires less power consumption, its use reduces driving voltage, and offers prospects for energy saving. Also, network level & equipment level technologies, not identified in this Recommendation, have potential for energy saving in future. For further energy saving, further increase in the speed and the capacity of transmission lines in the future will require improved performance of special types of memory that are high-speed, high-capacity and consequently, high power consumption such as SRAM and CAM (Content Addressable Memory) for buffering and routing.

- **Classification of Individual Technologies:** Table 8.5 shows the classification of individual Technologies in terms of their applicable levels and approach.
• 4.3.4 Possible Functions and Their Interactions

  o **Possible Functions:** In the previous clause, it was discussed that energy saving within networks has both the static as well as dynamic nature. Regarding energy saving, static nature shows how to construct the network with power devices, equipments, and network level technologies in the network design (pre-operation) phase. It minimizes the total energy consumption for the pre-assumed maximum traffic. To save energy, dynamic nature adopts the operation of device, equipment, and network level technologies to the various types of traffic in the operation phase and minimizes the total energy consumption.

  Static nature for energy saving is reflected by involving the technologies of the three levels (device, equipment, and network
levels) and is described as energy control process during the construction of the network. Dynamic nature for energy saving should involve the management process which collects the current statuses, analyses them, and conducts better procedure targeted at optimized operation. Management process is identified at each technology level, i.e., network, equipment & device level and it exists in every network node or server which oversees and manages the individual equipment of the network. Simple Network Management Protocol (SNMP) is an example of management process. To achieve network wide energy saving cooperation between different levels of management is required. Additionally, a database (for example Management Information Base MIB) stores energy related information which is necessary for the management.

Figure 4.5 shows functions generally applicable to any energy saving technology. These functions include database and their interactions.

![Figure 4.5: Possible functions](image)

As specified by the energy management function, the energy control and management function performs control actions to reduce energy consumptions and obtains status information. This function is
subdivided in to network, equipment &, device & level technologies. This function also collects basic information, calculates the optimum case of operation and issues operation commands to the energy control and energy measurement functions. Three subfunctions are included in it which are **DataCollecting** subfunction, **Optimization** subfunction, and **Operation** subfunction. Figure shows an information status base which is a database that gathers basic information of the current mode from the energy control and measurement function. A set of status information such as energy consumption and traffic is given by the status information base. The location of the functions and database is independent of the specific equipment.

- **Energy Control and Measurement Function:** The energy control and measurement function contains a control process and a measurement process which includes a set of various energy saving technologies. These functions are subdivided into device level, equipment level, and network level functions. Example of device level function is device clock change; example of equipment level function is node sleep operation; and example of network level function is routing path change as shown in figure 2. Energy control and management function is managed by the energy management function and is directly related to power consumption.

- **Energy Management Function:** In order to minimize total energy consumption, energy management function accesses the status information base and manages the energy control and measurement functions. Energy management function includes the following three subfunctions:
− **Data Collecting Subfunction**: This subfunction collects the necessary status information about the network nodes from the status information base.

− **Optimization subfunction**: In order to minimize total power consumption this subfunction decides which management operation should be performed on which network node.

− **Operating Subfunction**: This subfunction is used to send an operation request to the energy control and measurement function of a network node.

**Status Information Base**: This is a database for defining network node characteristics such as energy consumption and traffic by using a set of status information.

− **Combination Models of Energy-Saving Functions**: Combination models of energy-saving functions are shown in Figure 4.6 which shows three models: **local-loop model**, **global-loop model**, and **combined-loop model**. In Figure, the solid lines show the signalling lines (operation/monitor/access) and dotted lines show the data flow.
Local-loop model is usually deployed on a single network node such as router or a switch. In one node two principal functions and a database exist and the local control loop is closed in the node. Since the equipment level and the device level of the energy control and management function are executed in a single loop, the energy management function issues operation commands to these levels. Controlling the device clock according to the traffic is a typical example of this case.

Global-loop model is usually deployed on multiple network nodes and a single network server. The energy management function exists in a network management while the energy control and measurement function and status information base exist in each network node. Since the network level is executed among multiple nodes, the energy management function issues operation commands to the network level of the energy control and measurement function. Here, it is assumed that a network management server accesses and operates multiple nodes in a centralized manner. The
intentional routing which assigns the least power consumption route is a typical example of the loop model.

- **Combined-loop model** is usually deployed on multiple network nodes and a single network management server. In this model, the energy management function exist in the network node and network management server while the energy control and measurement function and the status information base exist in each network node. Both the global and local energy management function constitute two combined control loops. Combined control loop includes a local and a global loop and circulates among them. Since equipment level and device level of the energy control of the management function are executed in a single node, the local energy management function issues operation commands to these levels. Because the network level of energy control and measurement function is executed in a single loop, therefore, the global energy management function issues control commands to this level. In this model, each node performs self optimization in a distributed manner and the network management server accesses and operates multiple nodes in a centralized manner. Energy-based eouting is a typical example of this case where the global loop aggregates traffic route and the local loop puts the node to sleep when there is no traffic.

- **Impact Analysis of Energy Saving**
  
  - **Influence on Network Performance**: Aspects of network performance like the QoS & security may be influenced by energy-saving technologies. These energy saving technologies may use additional resources or processes. In another way, using unnecessary resources may be reduced. This may result in use of minimum resources such as minimum amount of equipment or minimum bandwidth. Here network performance could be degraded and could
cause increased delays, congestion, connection hang-up, and so on. Sleep mode technology, for example, can reduce energy consumption but if the wake-up time takes long, the communication delay may be increased. Thus energy saving technologies are realized as the trade off between energy saving and performance degradation. Therefore, energy saving technologies should be applied where network performance falls within the acceptable range for specific services.

The Shannon's capacity relationships, which are given below, are inversely proportional in phases of network planning, operation, and management (Chen Y. et al., 2011), (Li, G.Y. et al., 2011).

- Deployment efficiency v/s energy efficiency.
- Bandwidth v/s power, only in a given data rate.
- Delays v/s power.
- Spectral efficiency v/s energy efficiency, only in a given bandwidth.

While aiming to achieve energy saving with a guaranteed QoS, these trade-off relationships should be considered.

- **Influence on Service Provisioning:** Provisioning of a new service requiring extra capabilities and resources could result in increased energy consumption. Introduction of energy saving technologies along with the service provisioning can mitigate these consumptions. Provision of service increases traffic for the service, and additional resources are required which results in the increase of total energy. Introduction of the energy saving technologies simultaneously with the service provisioning will cause less energy consumption that the energy originally required without the energy saving technologies. For example, the compact base station with the small cell or relay station in the conventional cellular network with a macro cell are feasible to be established at the place of the urban
areas so that the number of the users' traffic demands can be achieved with less power, meaning that the energy saving technologies can mitigate the increase in energy consumption and improve efficiency. Therefore, when new services are provisioned, the benefits from energy saving technologies should be carefully evaluated. In any case of multiple simultaneous service provisioning, energy saving technologies should be applied so that the increased consumption should fall within the acceptable range in order to maintain individual service requirements (e.g., delay, loss, etc.).

- **High Level Requirements:** Compared to existing networks, networks with energy saving technologies allow network capabilities and their operations to reduce the energy consumption of the network. Following items support energy:

  1) **Approaches**

    a. It is recommended to reduce the volume of traffic to be forwarded by devices or equipments in order to save energy within networks.

    b. It is recommended to shift traffic at peak time in order to save energy within networks.

    c. It is recommended to control device/equipment operation according to traffic fluctuations for the purpose of saving energy within networks.

    d. It is recommended to forward traffic with less power by transmitting data in a simplified mechanism in order to save energy within networks.

  2) **Functions**

    a. It is recommended to support the energy control and measurement function, energy management function, and the status information base in order to save energy within networks.
b. To perform control action to reduce energy specified by the energy management function and to perform the measurement of energy consumption, the energy control and measurement function is recommended. Also, inclusion of device, equipment, and network level technologies are recommended.

c. To collect basic information, to calculate the optimum case of operation, and to issue operation commands to the energy control and measurement function, the energy management function is recommended.

d. To gather basic information of the current mode from the energy control and measurement function such as energy consumption and traffic, the status information base is recommended.

3) Influence on Network Performance

a. It is recommended that when energy-saving technologies are applied, the degradation of network performance should fall within the acceptable range for the services.

b. It is recommended that on application of energy saving technologies, the increased energy consumption caused by multiple simultaneous service provisioning should fall within the acceptable range in order to maintain individual service requirements (e.g., delay, loss, etc.).

- **Environmental Considerations**: Future network related energy-saving technologies which contribute to energy saving within networks in the future are reviewed and their impact analysed in this Recommendation.

- **Security Considerations**: As far as security is concerned, static energy saving technologies should not reveal any additional security risks because they do not have any interaction with the outside. But, as far as dynamic saving technologies are concerned, security issues can be raised because they are managed by outside functions. While introducing energy-saving technologies, these security risks should be considered for mitigating
security risks. Since the security risk depends upon the operation parameters of the cycle interactions among key functionalities, the parameters should be carefully selected.
4.4 New Identifiers in Future Networks

It is recommended in ITU-T Y.3001(2011) that FNs should provide a new identification framework which will help for intrinsic mobility support and optimal data access. The communication network objects such as users, data or contents, nodes, links, and communication sessions need to be uniquely identified in order to make it possible to select the proper combination of the functions they provide. An IP address identifies only nodes (hosts) in the application and transport layers and their locations in the network layer on the network topology. This is the main cause of the Internet’s inability to support mobility (Recommendation ITU-T Y.2015, 2009). Recommendations (Recommendation ITU-T Y.2022, 2011) and (Recommendation ITU-T Y.2057, 2011) specify the functional architecture for the introduction of ID/locator split functions in Next Generation Networks but they do not describe the architecture of IDs and their configuration methods. Therefore, to identify nodes, data, communication sessions, or services, new identifiers are needed in the upper layer protocols in future networks. Also, for data or contents, new identifiers should be defined so that a large volume of data can be efficiently accessed regardless of their location. Future Networks, in addition to new node IDs and data or content IDs, also need user IDs, service IDs, and location IDs. They also need new mapping or resolution systems for storing and providing dynamic relationships between different types of IDs.

Currently following identifiers are used in the Internet:

- Path: IP prefix.
- Network Attachment Point (NAP): IP address and/or MAC address.
- Node: IP address.
- Service and users: Uniform Resource Identifiers (URI) or Uniform Resource Locators (URL), email address, IP address, Network Access Identifier (NAI).

The current Internet supports only static bindings between the above mentioned objects, mostly by using static IP addresses. Since the number of network capable mobile devices such as laptops and smart phones has already exceeded the number of
fixed computers connected to the Internet, mobility will be dominant feature of the future networks.

### 4.4.1 Identifiers considered in FN-related projects

Various FN-related projects propose different types of identifiers:

- **MOFI project of Asia (Jung H. *et al.*, 2011)** proposed a host ID (HID) to be represented in two kinds of formats according to types of communications in which the first type is hierarchical HID for host based communications, for example, client-server and the second type is flat HID for general communications.

- **AKARI project (Kafle V.P. *et al.*, 2010)** has proposed to assign a unique name, i.e., human readable alphanumeric characters and ID, i.e., bit string to each host in the design of new generation network (NWGN) based on ID/locator split.

- **European Future Internet Project 4WARD [b-4WARD]** has proposed a network of information (NetInf) architecture based on an information centric paradigm which emphasizes making the information security functions independent of host authentication.

- **Named Data Networking (NDN) project of USA** proposes to assign a name to every data or content. It assumes hierarchically structured names, for example, a video produced by PARC may have the name `/parc/videos/WidgetA.mpg`, where”/” indicates a boundary between name components [b-NSF- FIA].

- **The Mobility First (MF) project of USA** proposes a common framework of globally unique IDs (GUID) which can be used to name users, devices, contents, contexts and so on [b-NSF- FIA].

Based on the above ongoing projects, identifiers proposed for FNs may be categorized as follows:

- **Human-readable IDs (such as content IDs))** which are composed of alphanumeric characters and non-readable IDs (for example, public key-based IDs).
• Hierarchical IDs and flat IDs.

### 4.4.2 Identification framework and General Architecture of Future Networks

Rectangular portion of figure 1 shows the identification framework of future network. It consists of four components which are:

1. **ID discovery service** – which discovers various types of IDs related to communication objects.

2. **ID spaces** – which define and manage various kinds of IDs. It contains **user IDs, data or content IDs, service IDs, node IDs, and location IDs** (NAP IDs or locators). User ID uniquely identifies the user in the network. A data/content ID is assigned to a data/content to identify a data or content independent of its location or owner. It enhances data security and is helpful for content mobility and caching in the different locations in the network. Service ID can be categorized into: **content service ID and network service ID**. The content service ID specifies an application service and associates its attributes such as the security keys, sequence numbers, and states. The content services IDs are mainly used by server and client nodes to identify the services. Data forwarding service provided by the network nodes is specified by a network service node. A network service ID may specify a logically isolated network partition (LINP) in network virtualization (ITU-T Y.3011, 2012), a virtual location area network (VLAN), or a particular protocol used for handling data packets. A node ID identifies physical or virtual device independent of its location in the network. A device or a node is assigned a location ID or locator to locate it in the network topology.

3. **ID mapping registries** – which maintain mapping relationships between various kinds of IDs. It stores and updates mappings between IDs and provides these mappings to the ID mapping services to achieve seamless services over heterogeneous physical networks.

ID mapping service – It performs mappings of IDs of one category with that of others. IDs of various types are used in different layers of protocols, for example, location IDs are mainly used in network layers while the other IDs are used by the application...
layers for the purpose of identification of various objects. Therefore, to store the ID mappings in the ID registries as well as to maintain the relationships between IDs of different categories and scopes, ID mapping services are required. ID mapping services also perform mappings of different types of IDs with their own specific networks. The ID mapping can be one-to-one, one-to-many, or many-to-one. The mapping relationship can be persistent or temporary, horizontal or vertical.

Figure 4.7: Identification framework in FNs

The above framework supports the unique ID space. It maintains relationship between some of the objects’ IDs. It too supports searching for IDs of target objects for communication.
4.4.3 Features of identifiers and their high-level requirements

Followings are the features of identifiers in general:

- The relationships between identifiers can be static or dynamic; the static relationship persists for longer time while the dynamic relationship may be short-lived.

- Identifiers can have flat or hierarchical structures. It is easier to search hierarchical identifiers from ID mapping registries than flat identifiers. In proliferation or generation of globally unique identifiers, the hierarchical structure is also helpful. But, on the other hand, the flat IDs provide more flexibility, persistency, and privacy.

- An object can be represented by different types identifiers. Alternatively, many objects of a given category or scope can be represented by the same identifier.

- Identifiers can be composed of bits or alphanumeric characters.

- Identifiers’ length can be fixed or variable.

Future networks have the following high-level requirements for identifiers:

- For ensuring reliability in network operation and communication services, the ID mapping functions are required to be accompanied by security functions.

- The identifier should have flexible structure because it would have enough space for further refinement and modification in case of new requirements on identifiers emerge in the future.

- There can be either static or dynamic mapping between two categories of identifiers. The static mapping relationship does not change as time passes while dynamic mapping relationship is allowed to change according to time or place.

- The identifiers should have features which can facilitate their mapping to other identifiers of appropriate categories.
The identifiers can be permanent or temporary. A permanent identifier can be associated with the same object forever or for a specific time period. A temporary identifier can be associated with the object for a short time and at time it may be dissociated from the object.

The identifier should clearly represent an object or group of objects of the given category and scope.

In a given scope, the identifier is required to be unique and the scope of the identifier can be local or global.

4.4.4 Environmental Considerations

The details of the environmental impacts is recommended to be discussed during drafting of future Recommendations that would describe specific IDs because the ID structure affects the design, implementation, and operation and maintenance of networks, and implicitly affects environmental impact of networks, although the relationship is vague and needs further study.

4.4.5 Security Considerations

Since identification is the basis for identifying different types of objects, any mistakes or malfunctions in the assignment of an identifier to an object, in mapping, or in any part of the handling of identifiers may cause various incidents such as system faults or security attacks, such as replay or leakage of privacy. Therefore, it is recommended that appropriate security considerations and countermeasures such as identity management (IdM) Recommendation (TU-T Y.2720, 2009)) should be considered in the designing, operating and maintenance of the identifiers. For example, while allocating or mapping identifies, it is recommended that the appropriate authentication mechanism be introduced. It is recommended for important identifiers that the certificates be issued or identifiers be made self-certifiable by using public key infrastructure, and that verification of the legitimacy of the identifiers be made be possible whenever and wherever necessary.