The Future of Intelligent Networks in Developing Countries

Martin Ngobye
Mbarara University of Science & Technology (MUST)

15

The Future of Intelligent Networks in Developing Countries

Narcis T. Rwangoga, ntrwangoga@cit.mak.ac.ug, and Martin Ngobye, mngobye@cit.mak.ac.ug, Faculty of Computing and IT, Makerere University

Telecommunication networks have become important not only for the academic community but also for users in business and industry. As globalization takes shape, this trend applies to both developed and developing countries. Unfortunately for many developing countries, the telecommunication networks are still dominated by the public switched telephone networks (PSTN), which are not able to support rising demand for services through networked systems. Innovative solutions have to be devised to plan, design and implement telecommunication networks that are able to seamlessly provide services demanded through the network today. This applies to both wired and wireless networks. The demand for network based services has risen in developing countries, considering how wireless technologies for cellular and personal communications have been extended to most areas in developing countries. Intelligent Networks (IN) is a promise that countries which are implementing telecommunication networks can use to deliver network based services. In this paper, we explore and discuss why IN provides the promise and requirements for their implementation. The objective is to provide a basis a tool for telecommunication network planers and implementers can use for IN structure implementation in developing countries where resources are highly constrained.

Introduction

Infrastructure for basic services has been expanding rapidly in developing countries. However this is not keeping pace with the needs, especially in telecommunications. Communication costs in developing countries are far higher than that in the rich countries. A number of countries have launched major plans for network expansion. Present telecommunication networks of the developing countries provide only basic service what is generally known as Plain Old Telephone Service (POTS). Manual and electromechanical switching is still extensively used.

All over the world, the term intelligent network (IN) is used to describe a network architecture that applies to all telecommunication networks according to J.M. Patel (1998) [1]. At the heart of this concept is an individual, software-defined communication profile for customers of telecommunication services. The IN combines important functions and data in a central location and provides them in only one or just a few nodes. The intelligent network provides an intelligent, distributed database access capability from a plurality of service switching points (SSPs) to data and functions stored in one or just a few service control points (SCPs) for the purpose of controlling the service according to D. P Satapathy (1998) [2]. In an intelligent network, the logic for controlling telecommunications services migrates from traditional switching points to computer-based, service independent platforms. This provides network operators an open platform provisioned with generic service components that can interoperate with elements from different vendors, based on published, open interface standards. This platform can be used to develop new and different services.

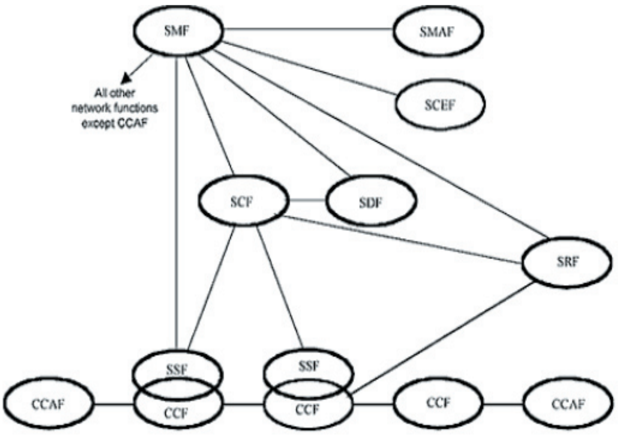
In developing countries, the traditional telecommunications environments still exist, where companies act both as network operators and service providers. D.P. Satapathy and J. M. Peha (1996) [3] define the network operator as the entity that owns and operates the network infrastructure. The same authors define the service provider as an entity that offers services to the subscribers. The service provider uses the network infrastructure of a network operator to deliver the service to the subscriber but is responsible for the management and development of the service. Service offerings are still likely to be driven by technological availability rather than customer need since with the traditional telecommunication architecture, most of the network infrastructure is based on proprietary interfaces with bounded capabilities. This environment results in long development times and large investments to deploy services. New technological capabilities, privatization and deregulation, and changes in market and customer demand have driven the need for new approaches to install networks. Operators and service providers need to add new features rapidly to attract and retain customers. Intelligent networks can play an important role in providing such new features and services.

The Intelligent network architecture

What we call the intelligent networks today has had its roots in the frustrations of network service providers with limited, highly specialized capabilities of the switching systems that were available when advanced network services first begun to be deployed in long distance network. Within traditional public switched telephone networks, the hierarchy of switching equipment and software must be upgraded each time a new service is added to the network. This is a complex and costly process. Further, network switches could not provide new number translation, routing and charging capabilities. As telecommunications services have evolved, the need to reduce the overhead for service use has increased along with the need to simplify maintenance and service upgrades or additions. The Intelligent network essentially separates these services from switching equipment and organizes a centralized system so that providers need not perform major modifications on multiple switches when they introduce new services. According to J. M. Peha (1998) [4], the first step in intelligent network development was to create separate service data in a centralized database outside the switching nodes. The second step was to separate the service programs, or service logic, and define a protocol that would permit the interaction between switching systems and intelligent nodes containing the service logic and data.

For service switching points and service control points (intelligent nodes) to work, common channel signaling, or out-of-band signaling is required as opposed to the traditional in-band signaling. Relying on out-of-band signaling, or signaling system 7 (SS7) protocols, provides the mechanism to place service logic and service data into dedicated network elements that can remotely handle call control and connection. SS7 also enables intelligent applications to communicate with other applications and to access databases located in various parts of the network. Certain network elements can be distinguished in every IN as shown in figure 1. Service switching points (SSPs) are stored program control switches that interface to the SS7 signaling network. The SSP embodies the call control function (CCF) and service switching function (SSF) entities.

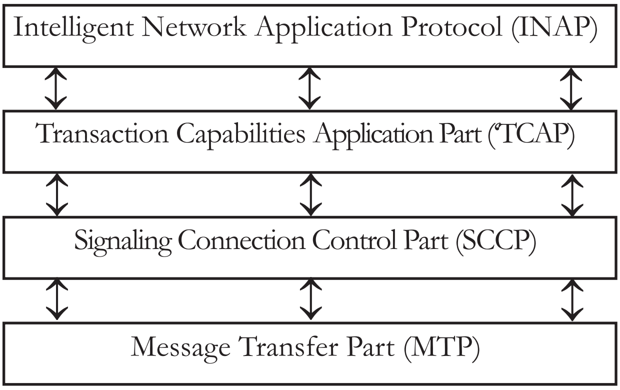
Figure 1. Intelligent Network Functions and Functional Relationships



CCAF	Call Control Agent Function
CCF	Call Control Function
SCEF	Service creation Environment Function
SCF	Service Control Function
SDF	Service Data Function
SMAF	Service Management Access Function
SMF	Service Management Function
SRF	Specialized Resource Function
SSF	Service Switching Function

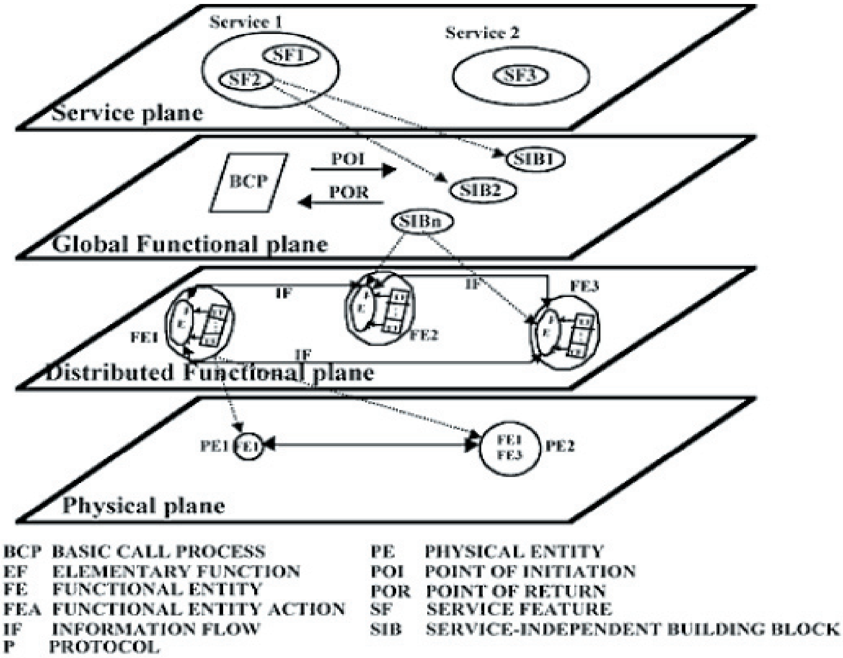
The SSF recognizes Intelligent Network service calls and routes the appropriate queries to the service control function (SCF) that resides in a service control point (SCP) via the SS7 network through signaling transfer points (STPs). STPs are high-capacity, high-reliability packet switches that transport signaling messages, using large routing databases, between the IN nodes. SCP commands are used by the SSP to process calls. The SCP is a fault-tolerant high capacity, transaction-processing entity that provides call handling information in response to SSP queries The Service Management Point (SMP) provides operation, administration and maintenance functions for the IN. The intelligent peripheral (IP) provides enhanced services or functions under the control of an SCP, possibly relayed by an SSP. As seen in Figure 2, the IN architecture is fundamentally based on SS7 and its protocol architecture. A common signaling transport capability known as the message transfer part (MTP) handles the corresponding open systems interconnection (OSI) physical, data-link, and network layers. The next level, signaling connection control part (SCCP), augments the MTP by providing both connectionless and connection-oriented message transport, as well as enabling addressing capabilities for message routing. The transaction capabilities application part (TCAP) provides procedures for real time transaction control. The final layer, IN application protocol (INAP) defines the operations required between IN network elements, such as SSPs and SCPs.

Figure 2: IN Protocol Stack


Intelligent Network Application Protocol (INAP)
Transaction Capabilities Application Part (‘TCAP)
Signaling Connection Control Part (SCCP)
Message Transfer Part (MTP)

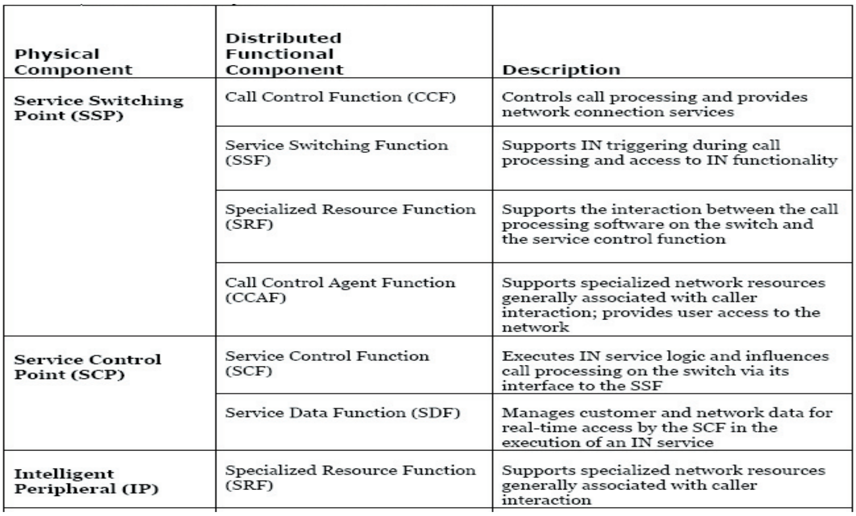
All of these basic elements form the infrastructure in Intelligent Network, which supports the notion of separating service-control functions from service switching functions, to realize more rapid services development and deployment. Another equally important concept in Intelligent Network has been the notion of service independence. Here, the primary goal is to identify and create generic sets of reusable service components that could be use to build new services and loaded into SCPs to generate new services rapidly. To provide a framework that would lead toward Intelligent Network engineering standardization, the Intelligent Network conceptual model (INCM) was developed (Figure 3). The INCM, which is solely a tool for describing IN capabilities and characteristics, is composed of four “planes” that represent different aspects of implementing Intelligent Network services. This model depicts the relationship among services and service features, global service logic, distributed service logic, and the physical network entities such as SCP and SSP. These planes include the service plane, the global functional plane, the distributed functional plane and the physical plane as shown in figure 3. The service plane describes services from a user’s perspective, where a service consists of generic blocks or service features that make up part or all of a service. The global functional plane deals with service creation and is comprised of the service independent blocks that will be used to create service features. Global service logic defines how service independent blocks are linked together to form features and how these service independent blocks interact with another basic service independent block known as the basic call process (BCP).

Figure 3. Intelligent Network Conceptual Model – (INCM) [Adapted from The International Engineering Consortium]

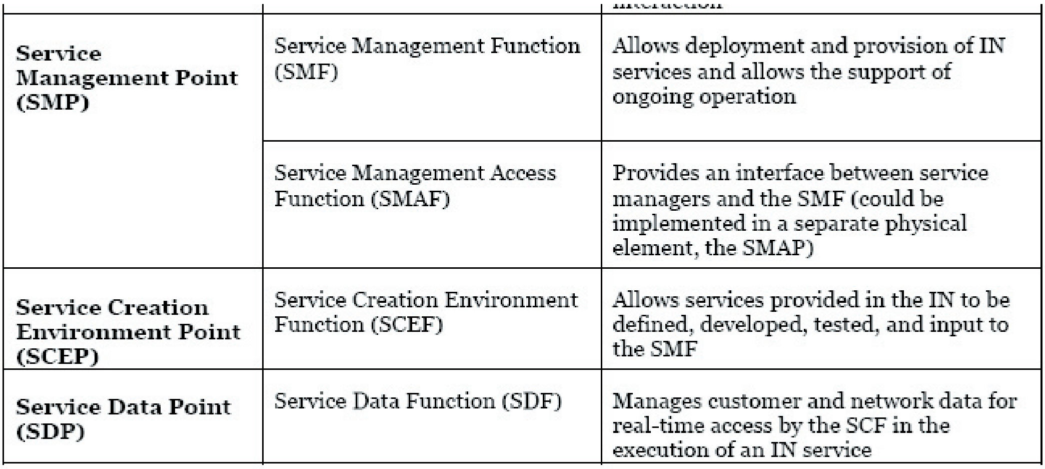


The BCP is the process that optimally supports services that do not require special features and is basic to the processing of all services. The distributed functional plane defines a set of functional entities that perform specific actions. Service independent blocks are implemented through a specific sequence of functional-entity actions performed by those functional entities. Table 1 describes functional-entity components as well as their relationship to the IN physical entities.

Table 1: In Physical and Functional Entities



Physical Component	Distributed Functional Component	Description
Service Switching Point (SSP)	Call Control Function (CCF)	Controls call processing and provides network connection services
	Service Switching Function (SSF)	Supports IN triggering during call processing and access to IN functionality
	Specialized Resource Function (SRF)	Supports the interaction between the call processing software on the switch and the service control function
	Call Control Agent Function (CCAF)	Supports specialized network resources generally associated with caller interaction; provides user access to the network
Service Control Point (SCP)	Service Control Function (SCF)	Executes IN service logic and influences call processing on the switch via its interface to the SSF
	Service Data Function (SDF)	Manages customer and network data for real-time access by the SCF in the execution of an IN service
Intelligent Peripheral (IP)	Specialized Resource Function (SRF)	Supports specialized network resources generally associated with caller interaction



		interaction
Service Management Point (SMP)	Service Management Function (SMF)	Allows deployment and provision of IN services and allows the support of ongoing operation
	Service Management Access Function (SMAF)	Provides an interface between service managers and the SMF (could be implemented in a separate physical element, the SMAP)
Service Creation Environment Point (SCEP)	Service Creation Environment Function (SCEF)	Allows services provided in the IN to be defined, developed, tested, and input to the SMF
Service Data Point (SDP)	Service Data Function (SDF)	Manages customer and network data for real-time access by the SCF in the execution of an IN service

The need for Intelligent Networks

According to a study conducted by Stanford University, USA, (1999) [5], it is reported that many scientists have predicted that a global network of affordable multimedia computers, online libraries, student-centered "learning ware" and enhanced human communications in general will improve access to high-quality education on a scale that simply cannot be accomplished today. But how are developing countries, where even traditionally laid network infrastructures are not yet fully in place, prepared to participate in the global network? Ever since the explosion of information technology took center stage in developing countries, more advanced research have been dedicated to provide network based services according to resources available. How will such networks match the rising demand for network based resources? Is it the time to consider pursuing more of intelligent network services and less on legacy network infrastructures? The network is the one element of the infrastructure that touches all others, from the middleware and applications to the servers and end users. It is, therefore, a logical place to implement changes that can cost-effectively scale to impact the entire networked system. When capabilities are administered at the endpoints, changes must be made at every distributed node or server, causing management complexity and operational costs to rise exponentially. If, however, these capabilities can reside in the network, where it is easier to centrally manage changes, they can scale more efficiently and simplify operations. Also, in this era of increased industry regulations and scrutiny of corporate governance, centralized management allows for better oversight and enforcement of business policy. For networks to truly become a reliable and cost-effective foundation from which to optimize business transparency and agility, they must not only hide complexity from the user, but they must also actively participate in the delivery of applications and services and be adaptive to the changing requirements of the business. The three elements of an intelligent networking strategy are a systems-level approach to network design, including how the network integrates with the rest of the information technology infrastructure; active participation by the network in the delivery of applications and services; and policies for linking business objectives and processes to network rules.

Implementation Challenges

R. Redford of Cisco Systems (2005) [6] identified a number of challenges for any one considering implementing an intelligent network. Redford gives three challenges in the paper titled "Enter the Intelligent Network".

The first challenge is at Systems-level. To date, the networking industry has tended to focus on solving customer problems one at a time, adding features, capabilities and intelligence only at the individual product level. With each individual product having its own management and feature design, the operation, management and maintenance of networks have become more complex and expensive as infrastructures have grown. This lack of a system-level approach has created technology islands and the need for additional components that can further increase complexity, add to operational costs and duplicate functionality. We now require a network that is more closely tied to, aware of and responsive to the needs of the applications, resources and devices connected to it. The increasingly complex tasks of intelligent IP networks will require more sophisticated functions, such as better content awareness, seamless encryption and filtering, greater quality of service and more adroit traffic shaping. These features can't be deployed as pockets of technology, but must be integrated throughout the infrastructure. System wide security, end-to-end performance controls, service-level resiliency and system wide management visibility can be achieved only by looking at the IT infrastructure as a highly integrated and open system, not as a series of interconnected boxes selected by product-level features and benefits. Some networking vendors are already taking steps in this direction by creating networking subsystems that tightly integrate the functionality of several previously separate components—router, switch, firewall, intrusion-detection/prevention system, wireless access point, IP telephony, etc. as one way of reducing systems integration costs and simplifying operations and management.

The second challenge concerns applications and Services. For networks to become more intelligent, they must be able to make better informed decisions regarding the handling of particular applications. An intelligent network can also enable applications to make better decisions. The network must not only look deeper into the payload of individual packets, to understand what type of application it is, and what it is trying to do; it must be capable of examining streams of packets as well. Already, with the adoption of Web services, traditional firewall technology, which focuses on packet-level network traffic alone, can't adequately protect the infrastructure. Web services using XML or SOAP, for example, require application-centric, message-level inspection to protect against this new level of vulnerability and should be an integrated component of any next-generation security solution. In the future, network components will be designed with intelligence that interacts with business applications to enhance their performance. For instance, an ASIC on a router could look into packet payloads from an order entry system during an order crunch. In this scenario, the network would understand what's happening in Layers 4 through 7. If it is the end of the quarter and the transaction server has orders piling up, the network could inspect packets to look for big orders from important customers with short delivery times, route the transactions to the appropriate server, flag the management system and create a follow-up transaction to ensure that the order was fulfilled on time. Of course, this scenario must be dictated by a business policy, which is why policy control is an imperative component of the intelligent networking strategy.

The third challenge is how to enforce policy. As mentioned earlier, the network touches every element of the infrastructure; therefore, it is in a unique position not only to monitor the transfer of information, but also to enforce policies in a very coherent way. Policy controls enable the network to be managed through policies and policy domains, creating a higher-level systems management capability that reduces risk of change as well as management and administrative costs. Linking network policy to business policy provides a framework to adapt the intelligent infrastructure to the specific needs of a particular business. It also has the potential to substantially reduce management complexity and therefore operational costs. For instance, an organization may have a security policy that states that all users must have the latest antivirus signatures and patches installed. But with thousands, or even hundreds of thousands, of endpoints to simultaneously control and monitor, this policy is largely unenforceable. However, the network, designed with a higher degree of interoperability between PCs, servers and policy appliances can automatically check when a new client wants to be connected to the network to see if the new device adheres to the organization's security policy. This example of policy-based intelligent networking already exists today through the joint efforts of leading networking and antivirus software vendors.

Services supported by intelligent networks

As developing countries are racing against their counterparts in the west, in closing the gap of unequal opportunities in technological advancements, the need for Intelligent Network services today are paramount. Most mobile networks have deployed services and yet many are yet to be accessed by customers. An intelligent network can be used to implement the following IN services, among other things:

(i) Roaming services: Mobility dictates a need for technology or standards that make it possible for different networks to talk to each other. Subscribers want to be able to use the same voice-activated services that they use in their own cities when they travel across boundaries.

(ii) Data-service Capabilities: Handset displays allow customers to use various message services. One, called short message service (SMS), works very much a pager. It allows phones to send and receive messages in addition to making or taking telephone calls. SMSs require many SS7 messages just to set up the signaling and the mechanism to get the data through the wireless network. It requires a significant amount of checks and balances, finding the database, pulling up the message, encapsulating it with the right header information to route it to the correct user, and finally sending it out like a phone call.

(iii) Multi-media: Video applications are new to enterprises. Until recently, the infrastructure needed to capture and transmit video reliably was prohibitively expensive. Advances in network infrastructure, capture devices, and playback platforms now make enterprise video a feasible alternative to meetings and company events. Innovative companies are finding new ways to use video technology for business.

Recommendations

There is need to analyze weak points in existing intelligent networks. There is also a need to test unimplemented network configurations as early as the planning stage so as to determine the configuration that has the best performance under given basic conditions. For example, the question arises as to how powerful the SCP or its individual processors must be or what capacities must be provided, and possibly in what form, for the individual services. The question also arises as to whether and how better performance can be achieved, possibly by changing the process management functions within the IN processors. A further critical element in operating an intelligent network is the overload protection mechanism which is supposed to stabilize the system as closely as possible to its performance limit. In practice, corresponding overload protection parameters can be determined only with great difficulty, which means there is a need to determine the optimum overload protection settings as a function of other network configurations and independently of network operation and to transfer them to the real network.

Conclusion

For a global network of affordable multimedia computers, online libraries, student-centered "learning ware" and enhanced human communications to become a reality in the developing countries, some decisions have to be made and a supportive environment created, including regulatory issues, choice of technology, cooperation with developed countries and support from international bodies. Developing countries have special opportunities and concerns regarding computer networking technology. They have a unique opportunity to leap frog into implementing advanced systems bypassing the older network. The IN provides a good opportunity of achieving this objective in a short time with very modest investments. However this needs a careful evaluation of the available technology options versus the needs. There is no doubt that IN would contribute to modernization of network based services in developing countries.

References

[1] J. M. Peha, "Tradable Universal Service Obligations," accepted to appear in Telecommunications Policy.

[2] J. M. Peha, "Spectrum Management Policy Options," IEEE Communications Surveys, Vol. 1, No. 1, Fourth Quarter 1998.

[3] D. P. Satapathy and J. M. Peha, "Spectrum Sharing Without Licensing: Opportunities and Dangers," Interconnection and the Internet: Selected Papers From the 1996

[4] D. P. Satapathy and J. M. Peha, "Etiquette Modifications For Unlicensed Spectrum: Approach and Impact," Proc. IEEE Vehicular Technology Conference, May 1998, pp.272-6.

[5]B. Lusignan, Afronet Telecommunications Plan", Stanford University, USA, 2005.

[6] R. Redford of Cisco Systems (2005) Technologies for Rural Communication", Workshop on Rural Communications", ITU/ICTP, Trieste, Italy, March2-6, 1995.

[7] M.V. Pitke, Opportunities for Wireless Technology in Expanding Networks", Proceedings of Workshop on \Computer Communication", Tata McGraw Hill, pp. 99-110, 1995.