

The Evolution of Intelligent Networks to Mobile and Broadband-Computers in the Network, Now and Tomorrow

Ray Crispin, Martin Sadler
HP Laboratories Bristol
HPL-95-68
June, 1995

Current Intelligent Network solutions will undergo considerable evolution to support the mobile and broadband networks of tomorrow. The present generation of Service Control Points, Home Location Registers and Intelligent Peripherals will give way to generic IN computing platforms which are capable of supporting a wide range of services. Requirements will develop over time, suggesting the need for highly adaptable computing solutions. Three key properties are needed to enable this adaptability: scalability, programmability, and modularity. This paper outlines the argument that a distributed, component oriented, approach will emerge to meet the needs of the future.

The Evolution of Intelligent Networks to Mobile and Broadband - Computers in the Network, Now and Tomorrow

1.CURRENT SITUATION

1.1 Digital Switching

Computer control of the telecommunications network started with the introduction of stored program digital switches in the seventies. Creating these systems has been, and continues to be, a very substantial engineering undertaking, with typical switches having 10-30M lines of code. Needless to say this poses huge software engineering problems, particularly with configuration management and regression testing.

It is interesting to note that much of the complexity arises from the need to manage the operation of the switches. Typical, 80-90% of the code is for management and only 10-20% to control the switching. Also, because of diverse world market conditions, there is the need to accommodate variations giving rise to the need for configuration.

1.2 Common Channel Signaling System 7

In the late seventies a major innovation was introduced which has proved to be key to the provision of current day telecommunication services. Common Channel Signaling System 7 (SS7) provides a telephone signaling channel which is separate from the voice path. SS7 greatly increased the volume of signaling information that can be exchanged between switches and opened up the possibility of having switches access other information services to control routing. Switch based services can only be implemented through a complex development cycle involving a very large code base. SS7 has dramatically expanded the possibility of using external processing and databases to offer new services.

1.3 Intelligent Networks

The first and most widely deployed service to exploit SS7 is the 800 service. When an 800 number is called the switch launches a Transaction Capabilities Application Part (TCAP) query via a Signal Transfer Point (STP) to a Service Control Point. The SCP applies some Service Logic, which can take into account location of calling party and time of day, among other variables, and refers to a database to select the number to which the call should be routed. The switch receives the response and routes the call.

Defining such an Intelligent Network architecture solves the most pressing service introduction problems while introducing new concepts and issues. The SCP is a highly programmable platform and to exploit its capabilities requires a means to rapidly create, test and deploy new Service Logic Programs (SLPs). A Service Creation Environment (SCE) is needed to provide service programmers with high level constructs to define service logic in application-oriented terms. By using Service Independent Building Blocks (SIBBs) a high degree of re-use can be achieved. Because of the risk of compromising the network, it is still an open issue to what extent SCE capabilities can be provided directly to telecommunications users, rather than the network operator.

Service Logic Programs rely on an internal information model defining which interactions with the switches are expected (or possible). Each switch Call Model has a number of interaction points (Trigger Check Points) at which external interaction can occur. The lack of

fully standardised Call Models, across equipment vendors and across international markets, undoubtedly complicates Intelligent Network solutions and the creation of service logic.

Services Nodes (SN) extend the SCP concept by supporting special circuit-related services, such as interactive voices response, automatic speech recognition and text-to-voice translation. Intelligent Peripherals, on the other hand, are controlled directly from the switches and typically are used to provide voice prompts ("enter PIN number") during service interactions.

Presiding over the whole family of Intelligent Network components is the Service Management System (SMS). The SMS is for managing the provision, operation and administration of services. Using the SMS the service provider can manage the lifecycle of their services, from development through testing, trial introduction, deployment, and eventually, withdrawal. Not surprisingly, the SMS may be extremely complex, especially if it has to cope with multiple and diverse types of service. The SMS itself could be regarded as a subsystem of the Operation Support System (OSS) of the entire network.

One major issue that has to be dealt with in introducing a new service is how to bill for it. Despite the machinery of SCPs, SNs, IPs and SMSs, if new services cannot be easily integrated into the business support systems (BSS), service introduction will be difficult.

1.4 Mobile Networks

Though SS7 was pioneered in the wireline network, the Global System for Mobile telecommunication (GSM) builds on SS7 and many of the concepts of Intelligent Networks. Completed in the late 80s, GSM standardises the services, functional subsystem interfaces and protocol architecture for personal mobility.

GSM defines a number of network computing elements that are used to perform the functions of call control and mobility management. The Home Location Register (HLR) keeps track of the mobile subscriber's location and service profile information. The Visiting Location Register (VLR) maintains the same information for subscribers who are roaming, and is frequently implemented as part of the Mobile Switching Centre (MSC). The MSC controls call handling and coordinates the handover of the connection from one Base Station Subsystem to another.

The Authentication Centre (AuC) supplies the mechanisms for ensuring the security of subscriber identities and for encrypting the radio channels. The Equipment Identity Register (EIR) is used to identify unauthorised equipment (e.g. stolen handsets).

A GSM network can be considered to be a special case of an Intelligent Network. The functional entities have ascribed roles which have analogues in the IN architecture and the interfaces are provided by Mobile Application Part (MAP) protocol which uses TCAP.

From the software development point of view, computing elements such as SCPs and HLRs require in the range 500-2M lines of code. Thus, though simpler by an order of magnitude than software-based switches, software development is still a major exercise. Further economies must be sought by re-using even smaller function pieces, particularly if by doing so new services are rendered easier to define and introduce.

2.DRIVERS AND THEIR IMPLICATIONS

What happens to telecommunication networks in the future is of concern to many parties: the operators, network equipment providers, computer manufacturers, systems integrators, software houses, consumer electronics companies, the entertainment industry and even the end users. We concentrate here on the network operator's viewpoint, and consider a number of drivers that will influence, though not necessarily completely determine, the direction in which network intelligence will evolve. Some drivers are concerned with the major demands for increased service from the networks and others are concerned with how we think the operators would like to go about meeting those demands.

2.1 Number Mobility and Portability

The completion of a call to a mobile phone demands a database lookup in order to determine the location of the receiving piece of equipment. But its not only mobile telephony that makes such a demand. "Numbers for Life" (e.g. 700 services) that offer the freedom to change location without the need to change area code, and numbers that could allow one to change service provider or operator without a change in number, both place similar requirements to perform lookups before terminating calls. Also, some users will want numbers that they can use across national boundaries. Once lookup processing is involved it is easy to see further services being added. We fully expect the percentage of "IN-calls" to rise from today's 5-10% of all calls worldwide to nearer 95%. Essentially this means that every call will involve some kind of additional processing.

Different operators and national groups of operators are likely to address the lookup problem in different ways. There are various architectural schemes to meet the needs of number portability, ranging from attaching small adjunct computers to each local switch to having a single large centralised computer, and various hybrid solutions. Because the characteristics of each solution varies, there is no reason to expect that the answers for different parts of the world, such as Hong Kong and the United States, will bear much in common.

So we can expect a demand for a range of network intelligence solutions that scale in at least two dimensions: the size of the database and the required throughput. Neither of these parameters will remain constant throughout the lifetime of the system. The database size is roughly determined by the product of number of subscribers and the amount of data kept per subscriber. At minimum the data kept for each subscriber will consist of a single number, but the demand to support a richer class of services, needing a user profile, will increase the amount of data considerably. The data may be kept in more than one place in the network. We would expect requirements to range from 10K to 100M subscribers, with from 10 bytes to 10K bytes per subscriber profile and a throughput of from 10 calls per second to 10K calls per second.

2.2 Integrated Services for Organisations

Currently many large organisations use Virtual Private Networks (VPNs) to support their communication needs and smaller companies use either 800 services or computers connected to their PABXs to provide such services as Automatic Call Distribution (ACD). The demand for increased integration of information and communication services will grow. For example, hospitals will want to link pagers, mobile phones and laptop computers across not just one campus, but maybe several, as well as other parts of the local community. They will want broadband access to large amounts of data, such as X-rays made at other, specialist, hospitals.

The Service Logic Programs associated with VPNs and Virtual Organisations could be very complex. This suggests that several levels of programmability need to emerge. End-users need to be able to customise their services, possibly integrating their personal services with those of the organisations to which they belong. Organisations need to be able to customise services and perhaps impose policy. Service providers need to support organisations and provide them with the underlying capabilities. This increasingly rich communication service world places major requirements on the way that Network Intelligence is provided.

2.3 System Convergence

Computer-based systems used by network operators are currently grouped under headings such as "Intelligent Networks", "Operation Support Systems" and "Business Support Systems". However, there are reasons to believe that this separation is awkward, and will not be maintained for long.

Services associated with personal users (such as call forwarding, and time of day routing) will need to operate and be managed in a common way across both wireline and wireless networks. It is not likely that customers will tolerate for long having to specify service options twice, in two different ways, for two different networks. As more users have mobile as well as wireline phones this problem will grow.

Customer care and billing systems need to be compatible across both the wireline and wireless networks. Customers don't want to receive two bills from the same operator, and operators do not want to manage duplicate customer information.

There are strong advantages to establishing a system which integrates BSS (customer care), OSS and IN/Mobility functionality. By having the appropriate linkages between these subsystems, a responsive, customer-facing, business system can be an important competitive advantage. So, whichever system architecture is adopted in the future, it will need to smoothly accommodate the convergence of all these functions.

2.4 Overlay Networks

When introducing new Intelligent Network functionality there is a clear need not to compromise existing networks. Overlay systems provide a way of introducing new services with minimum disruption, by attaching new elements at points in the network where it is easy to connect and easy to monitor the service. Usually overlay systems "intercept" certain calls for additional processing. Once the new service is accepted, and its impact on the network understood, a second generation implementation can look at a "deeper" integration with the underlying network.

Having already purchased a system to provide a service, operators tend to want to continue to use the system in the new, more deeply integrated, role. The Network Intelligence platforms need to be sufficiently flexible to admit such redeployment. This might require some changes in connectivity, requiring the support of a different protocol, but it is very desirable to avoid having to re-implement the service completely.

2.5 Growth of a Service

There are many unanswered marketing questions about which services consumers will really value and how much they will pay. This is particularly true in the area of home broadband networks, for which a large number of service trials are underway. Because of this uncertainty, it is very attractive to service providers to be able to introduce services on a trial

basis. If the services are taken up, the commercial pressure is then to deploy them much more widely. The clear requirement on the underlying computing platforms is that are both flexible (to permit experimentation) and scaleable (to support growth in use of successful services).

2.6 Constraints on Service Introduction

Whenever they are able, operators will seek to establish a greater degree of control over their capacity to compete. Most operators are currently quite constrained by the infrastructure provided by equipment vendors when it comes to introducing new services. Appropriate open, and worldwide, software standards for Network Intelligence need to be established. Effectively the impetus towards open computing systems needs to be translated into the world of Network Intelligence.

3. COMPUTING PLATFORMS

These factors have many implications for the way in which Network Intelligence is provided in the future. Here is a summary of our conclusions.

3.1 Industry-Standard Hardware

The proliferation of computing, fueled by the rise in ownership of PCs and the emergence of RISC-based client-server computing, has created a world market for processor power. It is reasonable to project that the massive world market will continue to drive the price of processing down, and enable the most widely used processing hardware to make major inroads into the markets of more specialised computing technologies. It is also well established that the price/performance of industry-leading processors will continue to improve at the current high rate for the next 10-20 years. At the same time, the investment required to sustain a world-leading position in processor technology continues to rise at an alarming rate. Finally, operators would, in the main, strongly prefer industry-standard, open, solutions.

The same arguments apply, in essence, to operating system technology. All these factors make it very difficult to envision specialised processor technologies or operating systems playing a significant role in providing Network Intelligence in the next century.

3.2 Continuous Availability

It is not sufficient simply to deploy computing technology from the office environment into the telecommunications network. Society has high expectations of the operational reliability of telecommunications systems, and the consequences of failure are dramatic. Though industry-standard hardware is increasing reliable, much of the software is not. It is essential that technologies are developed to enable dependable systems to be created out of ordinary components.

Given the argument for industry-standard hardware and operating systems, the solution will lie in a software-based approach to providing continuous availability of telecommunication services. The vision is of a network of processors, perhaps in geographically separated groups, with a scheme for replicating the processing associated with Network Intelligence. The network connections are engineered to avoid a single point of failure. Dependence on any one processing node is eliminated, effectively masking both hardware and software

failures. Not only does the processor network provide continuous service, but it may be repaired or upgraded without taking it down. Thus operators' requirements for (effectively zero) downtime and long service lifetime can be met.

Fulfilling this vision requires a series of complex technological problems to be solved, especially since a number of requirements must be satisfied simultaneously. Continuously available service has to be provided within the real-time constraints of call processing. Very high throughputs have to be sustained, especially as more and more calls require some sort of IN processing. The processor network itself has to have acceptable scaling properties. This means that over a defined range of number of processing nodes, as more processors are added an acceptable increase of overall processing power is achieved. Finally, the whole scheme must be capable of being managed as processing nodes are added, maintained and withdrawn, and as new services are deployed.

Technologies which solve some of the individual problems already exist, so we are confident in predicting that software-based solutions for continuous availability will prevail.

3.3 Generic Middleware

We have argued that future Network Intelligence solutions will be based on industry standard hardware and operating systems, with software technology being used to provide continuous availability. This layer of software, which mediates between the network element software and the operating system, is often called Middleware. The Middleware will contain, or at least work closely with, the software mechanisms to support continuous availability.

Though various software technologies have been used to create today's network elements, it is clear that object-oriented techniques will dominate in the foreseeable future. Therefore the Middleware layer will need to support object oriented software development. While it is perfectly possible to use object technology to create an application on a single processing element, several of the major demands suggest that a distributed approach will become commonplace. The need to support the convergence of previously separate systems argues both for a distributed system, since the applications will not all run on the same processor, and for a common software development environment. Industry standards are emerging in this area, such as the Telecommunications Information Network Architecture (TINA). [1] One coming from the computer industry that we expect to be very significant is the Common Object Request Broker Architecture (CORBA) from the Object Management Group. [2]

Because software represents such a major investment, which has to be preserved over time, there will be great impetus for the telecommunications industry to adopt worldwide, commercially supported, distributed object technologies.

3.4 Distributed System Support

With services not necessarily being embodied in a single network element, but distributed over many such elements, a number of system-wide capabilities become important. For example, the capacity to carry out a complex set of management operations so that the system is changed from one well-defined state to another, will be vital. This distributed transactional capability is essential for the consistent deployment of Network Intelligence services.

From the operational perspective, even the current, more centralised, approaches to providing Network Intelligence, are very difficult to manage. New service introduction is a painful process. In the future, the goal must be to increase the capacity of the operators to introduce, manage and control new services.

Thus underlying distributed computing mechanisms will need to be developed and specialised for application to Network Intelligence.

3.5 Component Based Network Elements

As much as possible of the foregoing technology can and will be industry-standard and generic. Now, functionality specific to Network Intelligence needs to be considered. When all the driving factors are taken into account, we see the need to provide custom solutions probably built using telecoms-industry standard components.

Custom solutions will be needed because of the sheer diversity of operators' businesses, circumstances and strategies. The quality of those systems will very much determine their capacity to compete effectively in providing services. However, there will also be a strong tendency to try to use re-use building system blocks to reduce the development costs and increase time-to-market of the solutions. Such building blocks will be provided by both the traditional network equipment providers and the computer industry.

So, over the next 10 years we expect to see a migration away from individual network elements such as SCPs and HLRs designed and implemented independently from each other. Network elements will be much more varied in nature and based on common components.

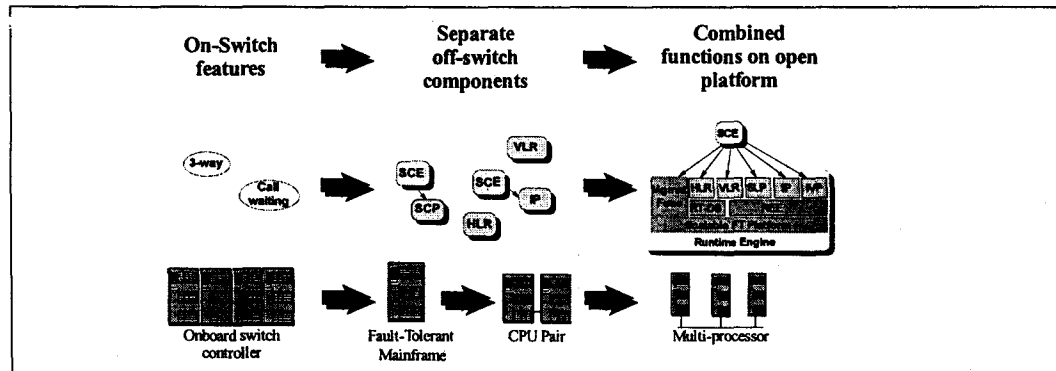


Figure 1. *Configurable Network Elements, Generations of Intelligent Network Element Platforms*

As in all transitional situations it is difficult to predict precisely which components will be found in the network element construction kit of the future; market forces will determine which components get commonly adopted. A strong candidate for an early component to emerge is an SS7 protocol stack, since interaction with SS7 is required by practically every intelligent network element.

3.6 Programming and Personalities

The different types of network elements in current systems were discussed earlier. Each can be thought of as having a particular **personality** which scopes the role it plays. However, network elements to support innovative services can be created by combining traditional personality types. For example, service functions supported by SCPs can be combined with location-based functions available through GSM. In future, many more personality types can

be expected. It is conceivable that software engineering environments will be used to develop and combine the common components, and simulate the behaviour of the new personality.

One driver for new personalities will be the convergence of mobile services and wireline capabilities. For example, operators may provide the **naming services** of such hybrid networks. Picture this scenario: participating in a multi-media conference call whilst at work, continuing with audio only on a mobile phone whilst on the car journey home, and finally finishing on the PC at home. Ideally one would like to be able to hand-over the call from one device to another without having to have set up the hand-over at the outset, and with little more action than saying "I'm now here" when picking up the new device. Not only are lookups required during call set up but the various multimedia objects associated with the call might also require re-direction. Such a service will require a new personality of network element.

3.7 Service Creation

Some personalities of network elements effectively have the service aspect more or less hardwired into the software. For example, a GSM HLR has only a very limited facility for modifying the service provided. Other elements, such as SCPs, are much more inherently programmable. When completely new personalities of programmable network elements are constructed out of components, corresponding service creation environments will be needed.

Service Creation Environments often attract attention in the industry, and offer the most apparent way for competitive differentiation. For this reason, we think they are unlikely to become standardised.

4. CONCLUSIONS

We have argued that the present landscape, where intelligence is embedded in switches and major IN functional nodes, such as SCPs and HLRs, will evolve in the direction of much more diverse and lightweight distributed functionality. The main drivers will be the need for flexibility and responsiveness in introducing new services, such as those required to support mobility and number portability.

The new network elements will, we believe, be based on open, industry standard, distributed computing platforms. Network elements will be built from a kits of reusable parts, enabling highly customised solutions to be created quickly and economically.

Finally, if operators are to compete on the basis of intelligent services, the full range of open Network Intelligence technology must be brought into play. Those operators who can work with their suppliers to create a future-proof infrastructure, and populate it with a rich set of services that can be easily enhanced and extended, will have a strong competitive advantage.

REFERENCES

- 1) TINA Reference, F Dupuy G.C. Nilsson, Y. Inoue, "The TINA Consortium :Towards Networking Telecommunications Information Services", proceedings of 15th International Switching Symposium (ISS'95), Berlin, April 1995.

- 2) CORBA Reference, "The Common Object Request Broker: Architecture and Specification, Revision 2.0", Object Management Group, 1995.

Biographies

M. Sadler received his B.Sc. in pure mathematics from Adelaide University in 1978. After spending 6 years at Imperial College, London, he joined Hewlett Packard Laboratories in 1989. He is Manager of the Intelligent Network Platform Department.

R. Crispin received his B.A. from Cambridge University in 1971, and his Master's degree and Ph.D. from Nottingham University in 1972 and 1975 respectively. He joined Hewlett Packard Laboratories in 1987 and is currently Director of the Intelligent Networked Computing Laboratory.