Providing Integrated Service Access

Part 2 – Management

A White Paper from

Inalp Networks Inc
Meriedweg 7
CH-3172 Niederwangen
Switzerland

http://www.inalp.com

Contents

1 Executive Summary

The capital cost of introducing any new service is often the figure that attracts attention. However, with multi-service provision, the initial equipment costs can be exceeded by the operational costs within a few months. Because customers are keen to take advantage of the inherently flexible nature of the service being offered, changes and reconfigurations are more common than with a conventional single service, thus potentially increasing operational costs.

Intelligent tools embedded in the centre of the network and manual intervention at the edges of the network have been the basis of many management processes. Intelligence and complex management functions are now migrating towards the edge of the network, reducing the degree of manual intervention needed but increasing the complexity of the management systems. In a multi-service network, some functions must be placed at the customer's premises. However, the flexible nature of an integrated network means that the functions at the edge of the network require more configuration and monitoring than would be needed with simpler network terminations such as those used for ISDN and ADSL.

If the service provider is to be able to supply a reliable, cost-effective service, then automated provisioning and customer control of their own service profile, supported by good remote configuration, diagnostic and maintenance tools is essential.

It is therefore very important to consider the management systems that are associated with integrated multi-service networks. Inalp Networks have studied the management issues in depth and this paper presents an overview of our approach to these issues, and how this can present service providers with new opportunities.

The paper looks at the general management system environment and then considers the different facets of management, such as:

- provisioning,
- configuration management,
- alarm and performance management, and
- software upgrades

It discusses the issues associated with each of these and describes how Inalp Networks believe that these issues can best be tackled. In doing this, we have taken a holistic approach to integrated multi-service networks. There are many boxes available on the market which allow multi-service provision. Many of these are excellent stand-alone devices but make very little provision for being managed as part of a network. However, Inalp Networks is not merely delivering a box but is creating and delivering a service delivery platform. This recognises that the integrated access device (IAD) must be supported by good management tools and concepts if it is to enable cost effective operation of complex service bundles.

Inalp Networks believe that our approach provides the optimum solutions to many of the management problems facing service providers. As your partner for the future evolution of integrated service delivery, we would be happy to discuss any of our solutions in more detail. The Inalp Networks web site (http://www.inalp.com) also contains more detail on Inalp Networks' technology and products and describes a number of practical examples of their application.

2 Introduction

The capital cost of introducing any new service is often the figure that attracts attention. However, as with conventional networks and services, the ongoing operational cost of providing access to integrated services is a major factor which also has to be taken into account. Indeed, with multi-service offerings, the operational costs can exceed the initial equipment costs within a few months. This is largely due to the inherently flexible nature of the service being offered, this flexibility being one of the major advantages that differentiates integrated services from conventional service offerings. Customers are keen to take advantage of this flexibility and, therefore, changes and reconfigurations are more common than with a conventional single service.

The management of services has historically been based on a combination of intelligent tools embedded in the centre of the network and manual intervention at the edges of the network. This has been matched by the intelligence used to control calls also being embedded in the networks rather than being at the periphery. However, intelligence and complex management functions are now migrating towards the edge of the network, reducing the degree of manual intervention needed but increasing the complexity of the management systems.

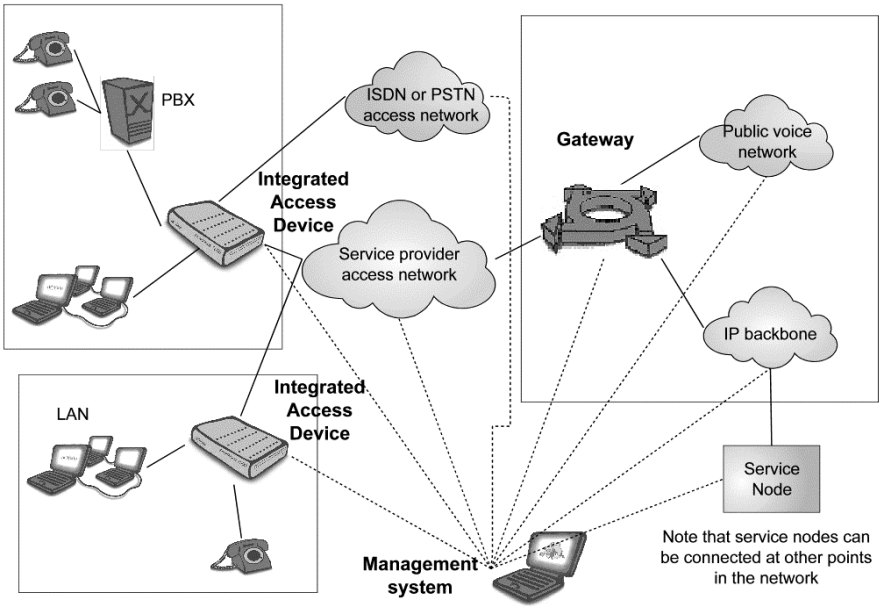

Figure 1 - a simple view of an integrated multi-service network

In a multi-service network, some functions must be placed at the edge of the network (ie the customer's premises). These include management of the bandwidth bottleneck (caused as increasingly high-speed LANs interconnect over an increasingly high-speed backbone network), service adaptation and interfaces to legacy systems. The companion paper to this, "Providing Integrated Service Access – Part 1 – Services", gives more information on the architecture which supports IP-based multi-service provision. The flexible nature of an integrated network means that the functions at the edge of the network require more configuration and monitoring than would be needed with simple layer 2 transmission network terminations, such as those used for ISDN and ADSL. If the service provider is to be able to supply a reliable, cost-effective service, then automated provisioning and customer control of their own service profile, supported by good remote configuration, diagnostic and maintenance tools is essential.

It is therefore very important to consider the management systems that are associated with integrated multi-service networks. Inalp Networks have studied the management issues in depth and this paper presents an overview of our approach to these issues, and how this can present service providers with new opportunities.

3 The cost of management

The cost of managing a network can easily be greater than the initial cost of the equipment. This is even more true of integrated multi-service networks than of more conventional networks.

The main factors which influence the management costs are:

- The cost of the network management system and its interfaces to the other management systems used by the service provider. This can be reduced by using standard interfaces and network management systems which are compatible with the service provider's existing systems.

- The cost of configuring new integrated access devices and making later changes to their configuration. If this has to be done by physically visiting each device, then the manpower costs (and travelling costs) can be extremely high. Ideally, newly fitted devices should be able to automatically install a basic set of parameters, and network management tools should allow any changes to the configuration to be automatically downloaded.

- The cost of service interruptions. A well designed network management system will ensure that any problems are identified, isolated and fixed as quickly as possible and with as little manual intervention as possible. Equally, the system must make sure that any problems with downloading new configurations or software updates to the integrated access devices do not cause a break in service. Service interruptions cost money to fix and cause customers to lose confidence in the supplier.

- The cost of network dimensioning. A network which is too generously dimensioned is wasting capital investment. A network which is under-dimensioned leaves users facing lost or interrupted calls and leads then to take their custom elsewhere. It is important that the management systems allow the performance of the network to be monitored without expensive manual intervention.

The factors described above have strongly influenced Inalp Networks' approach to network management. Our view of the issues which need to be tackled, and the solutions to those issues is described in the following sections.

4 The issues and the solutions

In the earlier sections of this paper, we highlighted some of the general issues which are associated with managing an integrated multi-service network. This section looks in more detail at the specific issues which face service providers and describes Inalp Networks' approach to solving them.

4.1 The management system environment

It is very rare for service providers to start deploying integrated services from a "green field". In the majority of cases, the service providers have evolved either from a long standing ISP business or from an even longer standing telephony service provider. This means that they already have a complex network in place and also have a correspondingly complex management system already in existence. This management system will include functions such as customer databases, backbone network management, RADIUS or TACACS servers, workflow management, service accounting and billing, customer relationship management, etc.

It is possible to create a stand-alone management system for the integrated service activities. This has the advantage that it is technically simple to achieve. However, it has the major disadvantage that it is completely isolated from the rest of the service provider's systems and thus causes problems in training, management, and data interchange and consistency. Although a few providers have used separate systems for trials and early in the service launch cycle this is not a viable long-term proposition.

The management system for integrated service access must therefore interface and integrate with the existing systems. This is not a simple task, because of the diversity of the systems which it must co-operate with, and this has often resulted in customised, expensive solutions being generated. However,

Inalp Networks believe that there is a better approach to integration. We provide compact, specialised management components to simplify or, in the best case, automate frequently recurring tasks. These provide an abstract of the underlying network elements and offer standard interfaces to the existing management system components. By using these specialised building blocks with standard interfaces, it is possible to keep the existing management systems and extend their functionality out to the new integrated services.

4.2 Provisioning

Providing service to a new customer is one of the most labour intensive activities in supplying any form of telecommunications service, and this is even more true when integrated services are considered. Not only is the provisioning activity expensive, but it is also likely to become a workflow bottleneck when demand is growing rapidly. This can lead to delays in providing service and, inevitably, generate considerable customer dissatisfaction.

Broadband transmission systems such as DSL or cable modems are now becoming available with built-in self-provisioning and autostart features, The service provider than simply has to ship the modem to the customer, who can install it himself and have instant internet access. Inalp Networks believe that it is important to extend this principal to integrated service provisioning and that the process must be independent of the underlying access transmission system. This independence from the type of transmission system is made easier by Inalp Networks' philosophy of designing integrated access devices (IADs) which can support service bundles over all of the common broadband access systems.

The primary objective, which is embodied in Inalp Networks' systems, is to provide a simple means of installing the IAD and establishing IP connectivity between that device and the management centre. The management centre can then take over the more detailed configuration of the IAD.

The following sections are based around Inalp Networks' IADs (known as SmartNodes) and their associated management software. However, the principles described apply to any integrated multi-service environment. The term Integrated Access Device can be taken to apply to any device that terminates an integrated multi-service access network.

4.3 Setting the initial parameters

So that this IP connectivity can be achieved, the IAD needs to have access to a basic set of parameters. For instance, the IP address assignment method (DHCP, PPPoE, Fix) and account information, such as the initial user ID and password, need to be available. This information can be pre-configured by the supplier before shipping the IAD to the customer, an easy-to-use graphical user interface can be provided, or an auto-configuration feature can be built in to the system.

Inalp Networks supply an auto-configuration feature which allows a new SmartNode to automatically connect to the management centre once it is physically connected to the network and powered up. This allows the whole process of configuring a new SmartNode to take place without any intervention on site.

In addition, Inalp Networks IADs come with SmartWare, which has a menu-based command interface, for carrying out local configuration of the IAD where necessary. Figure 2 shows the main menu of this system.

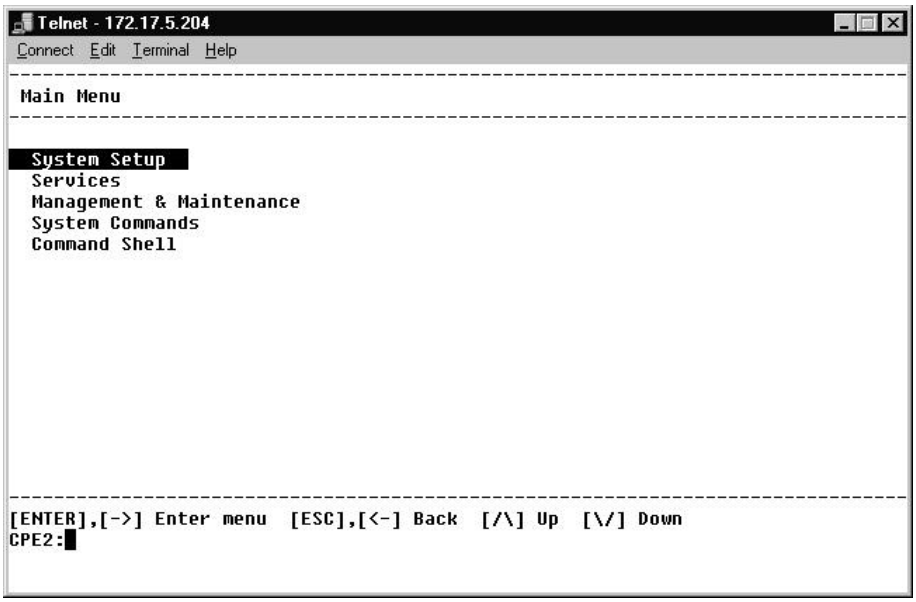

Figure 2 - SmartWare main menu

4.4 Subscriber Identification and the management database

Once IP connectivity has been established between the IAD and the service provider's management centre, the IAD needs to be registered and configured for the service bundle that the customer has subscribed to. Inalp Networks provide the SmartView Management Center to allow our IADs to be registered and configured. The architecture associated with this is shown in Figure 3. Although this illustrates the Inalp Networks solution to the problem, the architecture is one which forms the basis of any good service configuration system.

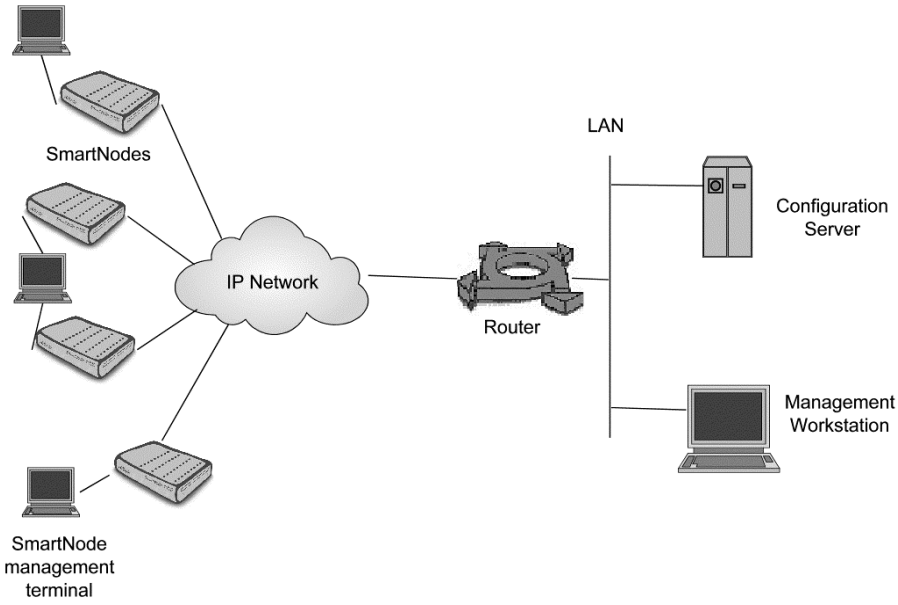

Figure 3 – SmartView management architecture

SmartView uses two main elements:

- A configuration server. This is a TFTP server which stores the configuration files for each of the SmartNodes installed on the network.

- A management workstation. This runs the SmartView Management Center application and communicates with the configuration server. This can be a normal PC.

In addition to these, the management centre contains other elements such as DHCP servers and local management terminals are provided for the SmartNodes.

4.5 Inventory management

An important element of the process is the management of the inventory, ie the data which describes the services which customers subscribe to and the devices (SmartNodes) which are connected to the network.

A customer will contact the service provider to ask for the provision of a new device, such as a SmartNode, or a change in its configuration. The customer care representative at the service provider will record the details of the customer, serial number and type of the device, and the services requested and set any device level parameters. The SmartView Management Center will then create a record for the device in the network and service views, if it is a new device, and a new customer record, if it is a new customer.

Network and service administrators can also create or make changes to the inventory in a similar way.

4.6 Node, network and service management

The configuration which has to be defined for an individual IAD consists of node specific settings, customer specific settings, service specific settings and network specific settings.

Network and service specific settings, in particular, will potentially apply to a very high number of nodes. It would be possible to set these up on a node-by-node basis but operational efficiency dictates that it must be possible to set the parameters once and then to define which group of nodes those settings apply to. An example of this might be a network which has its Quality of Service policy based on DiffServ codepoints which must be followed in the entire domain. A change in this policy would impact on every node in the domain. It is much better to have to only change this set of parameters once for the whole domain than to have to enter the changes for each individual node.

Inalp Networks' approach to this problem is to use configuration fragments to define particular parameters. These are then compiled into the overall configuration for the nodes. Thus, the configuration of a large number of nodes can be modified by simply making a change to the relevant configuration fragment.

Unfortunately, not all of the products on the market which support integrated networks provide this sort of capability and many behave as stand-alone devices which must be individually configured. Inalp Networks believe that this approach is potentially disastrous for any network which contains more than a few nodes.

4.7 Configuration management

Once the parameters have been set, the generation and delivery of the configuration files must be triggered.

The SmartView Management Center allows service providers to define network or service "instances", each of which has a number of IADs associated with it. For example, all of the IADs associated with one customer's network could be linked to a particular network instance, or all of the IADs which are registered for a particular service could be associated with a defined service instance. This simplifies configuration management by allowing network or service administrators to reconfigure groups of IADs by one set of actions rather than having to reconfigure them one at a time.

The network or service administrator selects the network or service level instance whose associated devices need to receive an updated configuration and invokes the Configuration Delivery Scheduler. The administrator can then choose the date and time of the deliveries. As an added level of security, to ensure that new configurations do not cause problems in the IAD, the Configuration Merger tool checks whether each device configuration has a complete set of values assigned to all parameters.

Customer care representatives can use the same tools to download the configuration for individual IADs.

As an enhancement, the Configuration Delivery Scheduler can automatically identify the devices with parameters which have changed since the last delivery. The administrator can determine the date and time of these automatic configuration builds.

4.8 Software upgrades

As well as the activities associated with providing service to customers, another critical activity which has to be handled by the management system is network-wide software upgrades. It is possible to manage these by distributing the new software on CD-ROMs and expecting the customers to install them. In a few cases, that may be the appropriate method. However, in most cases, that is a very time-consuming and potentially troublesome approach.

The growing complexity of the applications running on the IADs and the changing requirements being placed on the networks and the services have increased the need for regular updates. This has made the ability to manage remote upgrades of the software at each node in the network a key factor to be considered when looking at network management.

It has to be remembered that the upgrades are being carried out to nodes which are part of a network carrying live traffic. This means that the ability to download the new software is not the only consideration, even though it is clearly the fundamental one. It is also important that the timing of the installation upgrade can be scheduled, that there is a fallback mechanism to retain the service if the upgrade should fail, and that it is possible to monitor the progress of the upgrades from the management centre.

The Inalp Networks tools provided for our IADs not only allow the download of new configuration data from a central server but also allow software upgrades to be distributed to the IADs over the network from a central point. These downloads can be SNMP initiated under the control of the network management centre (or from the customer's site). To make sure that customers do not completely lose service if a software download should somehow become corrupted, the IADs have boot loaders to ensure that basic operations can still continue and that the full service can be then be restored. This is reinforced by the provision of facilities such as fallback to the previous working version of the software or firmware and the provision of SNMP traps so that the management centre can keep track of progress and of any problems

4.9 Job automation and scheduling

In some of the situations described above, a considerable amount of information may have to be passed around the network, for example in a network-wide reconfiguration. In some cases, such as software upgrades, there may also be a brief period in which the service is interrupted at individual nodes. It is therefore very important to be able to exercise tight control of the execution of these tasks if the network is not to descend into chaos.

The provision of good service management facilities, which can be monitored and controlled from a central point is clearly a prerequisite to exercising this control. However, it is important to schedule the tasks so that they cause as little disruption as possible for the users of the network. For example, scheduling upgrades to be carried out in the early hours of the morning (eg 2 am) is likely to cause the least disruption to the majority of users. Inalp Networks make this possible in our systems by building in a set of job scheduling tools to our network management system so that disruption to users can be minimised.

4.10 Alarm and performance management

In any network, alarm management is a very important function. It is essential that the network and services managers immediately become aware of any fault that is likely to affect service and that they are rapidly able to trace this to the unit which is causing the problem. However, it is not only faults that can affect service, but also any mismatch between the load being placed on the network and the capacity of the network. This mismatch may be because of some transient event or may be as a result of long-term

changes in traffic patterns. Whatever the cause, it is vital that there are good performance management facilities to enable these mismatches to be detected.

Many good tools and systems already exist for alarm and performance management, and these have been adopted by service providers. Any of these systems can only be as good as the information fed to it from the elements which make up the network and provide the service. Inalp Networks have therefore concentrated on making sure that our products provide a comprehensive set of SNMP traps and MIBs for alarm and performance management. By using the industry standard SNMP interface, we have also made sure that our products can be integrated into the existing management systems of service providers.

5 Conclusion

There are many boxes available on the market which allow multi-service provision. Many of these are excellent stand-alone devices but make very little provision for being managed as part of a network.

Inalp Networks is not merely delivering a box but is creating and delivering a service delivery platform. This recognises that the IAD must be supported by good management tools and concepts if it is to enable cost effective operation of complex service bundles.

Inalp Networks believe that our approach provides the optimum solutions to many of the management problems facing service providers. As your partner for the future evolution of integrated service delivery, we would be happy to discuss any of our solutions in more detail. The Inalp Networks web site (http://www.inalp.com) also contains more detail on Inalp Networks' technology and products and describes a number of practical examples of their application.

6 Glossary

DHCP Dynamic Host Configuration Protocol - a protocol that provides a means to dynamically allocate IP addresses to computers on a local area network.

DiffServ A means of prioritising different types of traffic in an IP network. The DiffServ concept is to aggregate multiple flows requiring a similar behaviour and thereafter deal only with these aggregate flows.

DSL Digital Subscriber Line - a means of providing broadband services over the standard telephony copper access network. The most common implementation gives up to about 2 Mb/s downstream and about 512 kb/s upstream.

IAD Integrated Access Device - used to provide an interface between equipment on the customers premises and an integrated (typically IP-based) access network.

IP Internet Protocol - a universally used protocol for communication over the internet.

ISDN Integrated Services Digital Network - the most widely used business telecommunications service across Europe.

ISoIP ISDN over IP - the Inalp Networks solution to providing all of the major features of ISDN over an IP-based access network.

MIB Management Information Base - a database of network management information used by the simple network management protocol (SNMP) standard.

PPP Point to Point Protocol - the internet standard for transmitting network layer datagrams (e.g. IP packets) over serial point-to-point links.

PPPoE PPP over Ethernet

RADIUS Remote Authentication Dial In User Service - a client/server security protocol created by Lucent. See RFCs 2138 and 2139 for more information on RADIUS.

SNMP Simple Network Management Protocol - a transmission protocol widely accepted as a de facto standard for network management.

TACACS Terminal Access Controller Access Control System - a protocol which allows a network access server to offload the user administration to a central server.

TFTP Trivial File Transfer Protocol - a commonly used protocol for transferring files across IP networks.