Providing Integrated Service Access

Part 1 - Services

A White Paper from

Inalp Networks Inc
Meriedweg 7
CH-3172 Niederwangen
Switzerland

http://www.inalp.com

Contents

1 Executive Summary

Service providers are finding it increasingly difficult to compete in the telecommunications market by differentiating their offering on price alone. A combination of regulatory and competitive pressures has forced the cost per minute of basic services, such as simple telephony, down to a level where further reductions cannot easily be achieved. Similar factors increasingly apply to the use of technologies which provide a higher bandwidth than POTS or ISDN. The infrastructure costs associated with providing new basic access services such as DSL are high, while the price which customers are willing to pay for services based on these technologies is low, and this leads to very low margins for the providers.

The simple provision of bandwidth is thus becoming a commodity market. As a consequence of this, service providers are finding that it is necessary to focus their attention on the provision of enhanced packages of services. This is leading to a split in the industry into access providers, who are dealing in a relatively low-value commodity, and service providers, who are supplying high-value service bundles.

However, basic economics still apply and it is important for the service providers to be able to reduce their costs by utilising a single infrastructure wherever possible, or by being able to introduce a high degree of commonality between the equipment used for different infrastructures (for example, by using the same basic access device to interface to a variety of access networks). In common with most industry experts, Inalp Networks believe that Internet Protocol (IP) based networks will be the way to provide integrated access for a wide range of services over a wide range of infrastructures. We have developed the technology which will make this possible and this paper describes how an integrated approach to service provision, using IP, can best meet the needs of service providers and their customers.

It considers how this approach can be applied to:

- Transmission independent service provisioning
- Providing telephony services
- Providing PBX networking services
- Providing internet access to business customers
- Providing virtual private network services
- Supporting Application Service Provisioning
- Supporting remote access and teleworking
- Integrating services

and outlines the Inalp Networks solutions to the issues raised in each of these areas.

Inalp Networks has put a lot of thought into how value-added service bundles can be delivered to the customer, because access is a key factor to the success and quality of the service. In this paper we show some of the pitfalls that a provider may face and how our products can support him to safely overcome them. The SmartNode Integrated IP Access Devices combine features found in enterprise routers with toll quality voice over IP and a focus towards scaleable deployment and operation. At Inalp Networks we are committed to building access products that can cope with the changing world of integrated service provisioning. 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

Service providers are finding it increasingly difficult to compete in the telecommunications market by differentiating their offering on price alone. A combination of regulatory and competitive pressures has forced the cost per minute of basic services, such as simple telephony, down to a level where further reductions cannot easily be achieved. A number of innovative pricing packages have been introduced by service providers in a bid to attract customers, but these only tend to be attractive to a sub-set of the overall customer base. Customers are thus becoming increasingly reluctant to switch supplier based on cost alone. Even in countries where costs savings can easily be achieved by moving to new suppliers, most customers have stayed with their existing supplier.

Similar factors increasingly apply to the use of technologies which provide a higher bandwidth than POTS or ISDN. The infrastructure costs associated with providing new basic access services such as DSL are high, while the price which customers are willing to pay for services based on these technologies is low, and this leads to very low margins for the suppliers.

The simple provision of bandwidth is thus becoming a commodity market. As a consequence of this, service providers are finding that it is necessary to focus their attention on the provision of enhanced packages of services, while buying in the bandwidth to support these services from established network operators such as the telcos and cable operators. This is leading to a split in the industry into access providers, who are dealing in a relatively low-value commodity, and service providers, who are supplying high-value service bundles. Service providers can differentiate their services from those of their competitors by adding value to the individual services, by increasing their quality, by providing a more comprehensive bundle of services, and by improving the flexibility in the service packages they offer.

However, basic economics still apply and it is important for the service providers to be able to offer this enhanced portfolio of services at a price that customers will find attractive, while still providing themselves with an acceptable margin. This means that they need to be able to reduce their costs by utilising a single infrastructure wherever possible, or by being able to introduce a high degree of commonality between the equipment used for different infrastructures (for example, by using the same basic access device to interface to a variety of access networks). Figure 1 highlights some of the diversity in access infrastructures which can now be found. Whatever the infrastructure used, it should be invisible to the customers, since they do not want to change the way they work simply because of the underlying network technology. Service providers also need to manage the provision and operation of their services in as efficient a way as possible if they are to achieve acceptable margins and customer satisfaction.

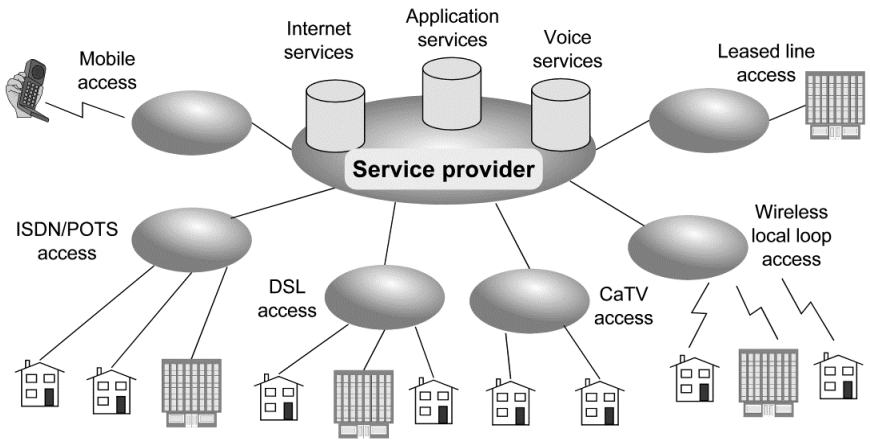

Figure 1 - Diverse services over diverse infrastructure[1]

1 This paper concentrates on broadband access – i.e. DSL, CaTV, wireless local loop, leased line.

The need for a wide range of services to be offered over an infrastructure which is invisible to the customer, but cost-effective for the provider, leads to the requirement to look at how converged services can be supplied on a variety of access and backbone networks. By matching the convergence which is taking place in LANs and PBXs in the customers' premises with convergence in the service provider's network, we can provide a seamless set of services from end-user to end-user.

In common with most industry experts, Inalp Networks believe that Internet Protocol (IP) based networks will be the way to provide integrated access for a wide range of services over a wide range of infrastructures. We have developed the technology which makes this possible and this paper describes how an integrated approach to service provision using IP can best meet the needs of service providers.

3 Why should service providers use integrated access?

The previous section described the background to Inalp Networks' decision to follow an IP-based integrated access path. But why should service providers follow this path?

Perhaps the most pressing need that many service providers have is to get out of the price war and to provide an attractive offering to their customers which is differentiated by factors other than its cost. The benefits of using IP in the backbone (or core) network have become apparent in recent years and most network operators and service providers have installed, or are installing, an IP backbone network. Although IP backbones were originally introduced to cope with the increase in data traffic, more and more operators are starting to use them to carry all types of traffic, including voice. By using the Inalp Networks approach, it is possible to extend the benefits of this IP core out to the customers - thereby creating an integrated, flexible infrastructure that can provide multi-service capability over a variety of existing transmission infrastructures (eg DSL, CaTV, leased lines etc).

The provision of multi-service capability is not, in itself, justification for following this route unless there is a real, and growing, demand from customers for such capabilities. There are a number of indicators which show that such demand exists. Two examples are:

- More and more companies, large and small, are beginning to appreciate the benefits of teleworking. This not only gives them greater flexibility in where their staff are located but also makes collaborative working between companies much more viable. Significant efficiencies can be introduced by the use of teleworking. However, for this to be happen, it must be possible to extend a wide range of services out to locations which are remote from the main sites.
- Application Service Providers (ASPs) are becoming appreciated for the freedom they can give companies from the continuous cycle of installing, maintaining and upgrading software. However, ASPs can only be used if good communications can be established between the users of the application and the ASP.

In both of these cases, Inalp Networks believe that the solution is to establish integrated access networks based on IP, since this is the only viable way of providing such services. The following sections of this paper will show how that is possible, and how this philosophy can be extended to other applications. It will also demonstrate that it is not necessary to abandon legacy systems (eg ISDN connections) or suffer any downgrade in quality in order to follow this path.

4 The issues and the solutions

The preceding sections have looked in very broad terms at the issues facing service providers in simply making services available to customers. This section looks at some of the issues in more detail. However, there are a host of issues which can affect a service provider, whatever solution they adopt, and it is only possible to give an outline of how Inalp Networks believe each of these issues should be addressed.

Inalp Networks have looked at most of the issues which could affect service providers and have developed solutions. As your partner for the future evolution of integrated service delivery, we would be happy to discuss any of these 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.

4.1 Transmission independent service provisioning

4.1.1 Diversification in access

The transmission media which are available to provide broadband access between customers and the backbone network (and hence other services) are increasing in their diversity. Commonly available technologies today include DSL, Wireless Local Loop (WLL), cable TV (CaTV) systems and leased lines. Service providers have to be able to cater for all of the major access technologies if they are to be able to choose the technology best suited to delivering the service bundle to the customer, or if they are to make use of technologies which customers are already connected to.

Inalp Networks have taken a two–stage approach to this problem. In the first stage, Integrated Access Devices (IADs) are used which provide an interface between the customers' premises equipment and the Ethernet interface which is commonly found on the network terminations of access networks (eg on cable TV modems). In a second stage, the IADs can directly interface to the transmission technology, for example by incorporating the functions of the cable TV modem in the IAD. However, this can only be done if the access and the service provider are the same company. Otherwise, the IAD and the transmission modem must remain separate, being part of different management and responsibility domains.

As well as interfacing to standard broadband connections such as CaTV and DSL, Inalp Networks IADs also support leased lines, since they are a major legacy access transmission system.

4.1.2 Remote provisioning

Efficient service provision relies not only on the ability to provide a connection capability which is independent of the transmission medium but also on the ability to configure (and re-configure) the system and to upgrade software without physically visiting every node in the network. A number of products exist for integrated access which have in-built remote management, upgrade and provisioning capability. However, if expensive manual intervention is to be minimised, it is important that any upgrade facilities are able to maintain the connection to the management centre if the process fails. In this case, the node can be reconfigured to restore service without a site visit. If these facilities do not exist, then service can only be restored by physically visiting the node. With the need for upgrades to track the rapid evolution in services and their supporting protocols, this can make management of a network very costly and difficult.

Inalp Networks meet this challenge by providing a network management system which allows remote configuration and management of the nodes in the network, as well as making software upgrades from a central location possible. Inalp Networks also ensure that effective fallback facilities are built-in to allow remote restoration if any upgrade fails. The companion paper to this, "Providing Integrated Service Access - Part 2 – Management", describes Inalp Networks' approach in more detail.

4.2 Providing telephony services

Although the provision of broadband services including audio and video is a major growth area, basic voice telephony is still one of the most important telecommunications services. No service bundle is complete unless it gives customers full support for voice telephony. By integrating voice into the services using IADs, it is possible to create a whole new area of differentiated services – such as least cost routing, unified messaging and PBX networking.

4.2.1 The ISDN legacy interface

Throughout most of Europe, ISDN is regarded as the business voice network, as well as being widely used for data transmission. Service providers must support this legacy since customers are used to its features and have invested heavily in compatible terminal equipment.

Inalp Networks have considerable experience in ISDN and have developed a profound understanding of its applications and technology. We have also looked very carefully at what is needed to ensure full interoperability between different types of equipment. The Inalp Networks IADs provide interfaces to ISDN customers' premises equipment which are fully compliant with the standards and can interoperate with a wide range of equipment. On the network side, Inalp Networks have developed the ISDN over IP (ISoIP) protocol, which is described in "Feature expectations" on this page, and ensures that ISDN users do not lose any of the features they are used to.

4.2.2 Quality expectations

"Voice over IP" (VoIP) is a service that has been much discussed, and much criticised. However, many people talk about VoIP when they are really talking about voice over the internet. Voice over IP is not the same as voice over the internet. While early applications of VoIP were tempting home users to call their Australian uncle over the internet, and put up with the limitations, the service providers of today recognise the need to provide good quality voice to business customers.

Service providers who are meeting the needs of business customers are investing heavily in IP backbone networks which support Quality of Service (by using techniques such as ATM, MPLS, DiffServ). Since they can provide Service Level Agreements on IP, these networks can support a variety of different services, such as Virtual Private Networks and Application Service Provision. These networks have a well defined internet gateway and internet access is one of the services offered on the backbone. Telephony is another one of the services which can be provided on this backbone. However, it is important to be able to take the service capabilities out to customers and therefore to be able to extend them beyond the backbone. Inalp Networks ensure that the QoS which is supported in the backbone is also enforced out to the customer premises. We also make sure that expected quality standards are met in the IAD and that the available QoS support in the backbone is used in the most efficient way.

This is achieved as a result of the real-time capabilities of our routing core - e.g. the node latency for a voice packet is well below 1 ms (as compared to the 5 ms which other routers may have for any packet). Such real-time response is not easy to achieve and it is an area of expertise that Inalp Networks has invested heavily in. Compliance with the QoS policy in the backbone is ensured by the IADs through the provision of features such as TOS and DiffServ labelling or mapping of IP traffic flows onto different ATM Permanent Virtual Circuits.

4.2.3 Feature expectations

Customers expect any new service package that includes voice to provide them with all of the features of ISDN which they have become accustomed to, in a way which they have become accustomed to. Any offering from a service provider has therefore to support the full range of ISDN features, such as supplementary services for voice and for data.

Inalp Networks has introduced a voice over IP signalling protocol (ISoIP – ISDN over IP) which is based on the industry standard H.323, but outperforms H.323 in speed and features. ISoIP is able to provide the complete range of ISDN supplementary services over an IP access network. We are also developing signalling solutions that comply with the next generation of fully IP-based carrier call control architectures and support the ISDN features.

4.2.4 Provider migration

The existing providers of telecommunications services have evolved their service portfolio and customer base over many years. A new provider of integrated services therefore faces considerable barriers when trying to break into this market, not least the customers' fear of moving away from a known supplier to a new unknown supplier – however good that supplier's offering may appear to be.

The route which provides most comfort to both the customer and the supplier is a gradual, controllable migration path from the old to the new. By initially providing the integrated service to selected call destinations, such as specific company sites and/or employees' home offices, the service provider can expand his offering as the customer's trust in him and his products grows.

Inalp Networks provide an IAD which contains sophisticated call routing functions and a local breakout path to the PSTN, as shown in Figure 2. This allows the old and new to live in harmony while this migration takes place. Using this migration strategy, it is possible to set up the IADs so that, for example, voice calls can still be received and/or sent via the existing PSTN connection and other calls can go via the IP service provider. As the customer gains confidence and migrates more towards the integrated IP service, these routings can easily be changed in the IAD so that more calls are sent and received via the IP service provider.

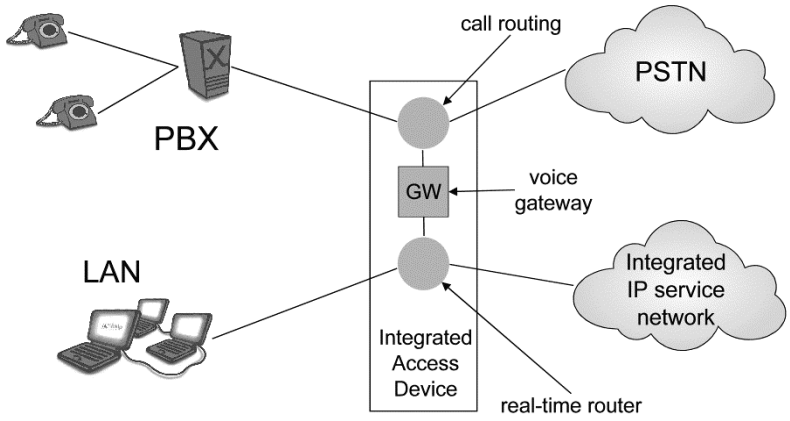

Figure 2 - migration from old to new networks

4.2.5 Carrier number portability

The configuration described above also solves a potential problem with number portability as customers move between carriers. Although it is theoretically possible for a customer to keep their existing numbers as they move between service providers, the process is in practice often fraught with technical problems and high costs. Since businesses cannot afford to change the numbers which people associate with them, they are often discouraged from moving to a new service provider.

Inalp Networks' approach to this problem is the configuration shown in Figure 2. This enables the new service provider to route outgoing calls over his network while still allowing incoming calls to reach the customer through their existing PSTN access.

There is also an issue with the use of CLI which arises in this situation. In general, CLI must not be provided if the extension which originated the call cannot be reached when calling back using this CLI. On carrier interconnection, the CLI may therefore have to be replaced or restricted. A prime example of this is an outgoing call over IP to a PSTN phone. The IP provider cannot use the CLI of the incumbent provider (because of the way that number portability is handled) and he cannot provide his own (because he may not be able to support incoming calls). Sophisticated CLI masking and translation functions have to exist in the IAD to ensure compliance with the rules for the use of CLI in networks.

4.2.6 Reconfiguring PBXs and adding trunk ports

An alternative approach to that described above is shown in Figure 3. At first sight, this has the advantage of using a simpler access device, since the existing PBX is used for access to and from the PSTN.

However, a major drawback to this approach is that the PBX has to have new ports added so that the Integrated Access Device and the PSTN can be connected to it. It also has to be reconfigured to cope with some calls being routed via the PSTN and some calls being routed via the integrated IP service network. The access device also has to be configured to handle the calls which it is routing. This duplication of two devices (PBX and access device) needing to be reconfigured is an ongoing commitment.

This is further complicated by the fact that the PBX is usually under the control of the customer (or an IT outsourcing company) whereas the Integrated Access Device is under the control of the service provider. This split of responsibility inevitably causes co-ordination problems.

Inalp Networks believe that the solution is to use the configuration shown in Figure 2. Additional ports do not need to be added to the PBX, since the existing ports are simply connected to the IAD. The PBX does not need to be reconfigured, since all of the routing intelligence is contained in the access device. This single point of intelligence makes ongoing reconfiguration much faster and much more controllable.

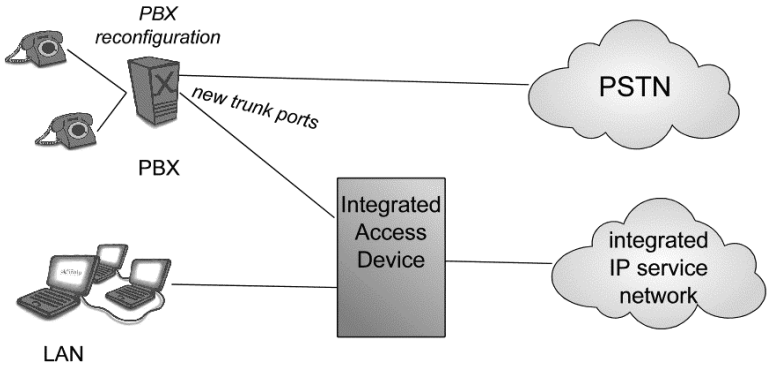

Figure 3 - alternative voice access using a PBX

4.2.7 Lifeline support

The reliability of integrated service networks is improving, but they still find it almost impossible to economically match the 99.97% uptime of the established PSTN. Power failures, congestion, route failures (eg the mechanical digger effect) all contribute to downtime. The PSTN has evolved over many years of development and investment to cope with these problems and no integrated service network has yet reached that level of maturity.

For many purposes, customers can accept a slightly lower uptime if this is traded off against a much more flexible and cost effective service. However, it is still important to make provision for basic calls, such as to the emergency services, with an uptime equal to the PSTN. In some countries, this is a legal/regulatory requirement.

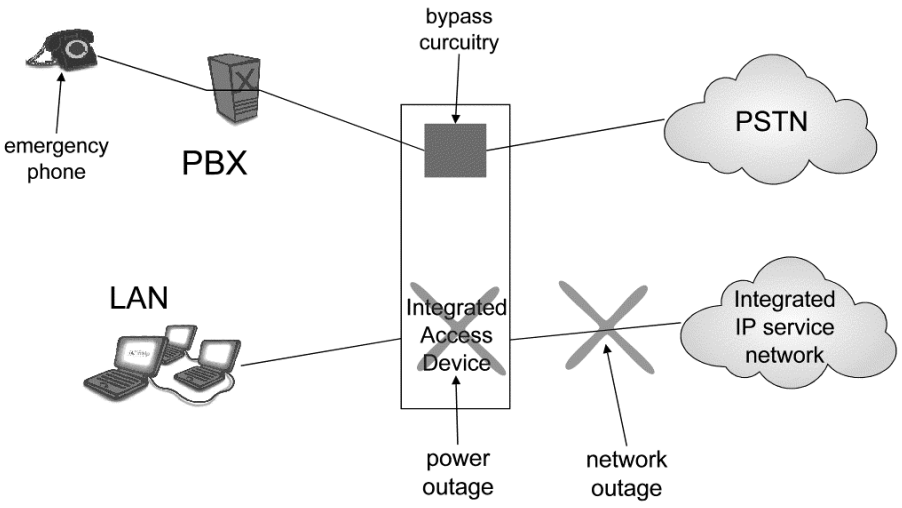

Figure 4 - lifeline access

Inalp Networks provide routing facilities in the Integrated Access Device which allow a basic PSTN service to be maintained when the integrated service is not available. This is designed so that even a total power failure at the customer's site will not disable the bypass circuitry.

4.2.8 Network evolution from V5.2 to SS7

The current telephony service is based on highly sophisticated, large and expensive switching and IN (Intelligent Networks) systems. Decades of refinement and billions Euros of investment have led to a familiar and reliable telephony system which is known to everybody.

Integrated service providers can use IP-based access over their integrated service networks to provide access to this infrastructure, thus taking advantage of a reliable legacy system. The best interface to use is V5.2, the standard access concentration interface to PSTN switches. This is illustrated in Figure 5.

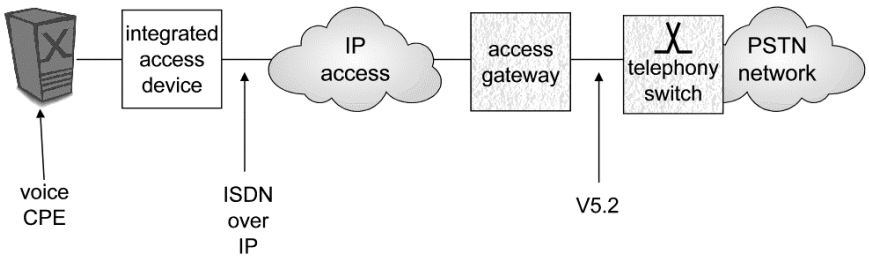

Figure 5 - V5.2 access to PSTN

In this configuration, all call processing, accounting, billing and network routing for telephony traffic is managed by the PSTN infrastructure, with the IP access simply acting as the transport medium.

However, many large PSTN networks are themselves migrating to an IP scenario. In these networks, call control, accounting, and IN services will be IP based, and will interface with the legacy world (including other carriers) through SS7. Although this is only really starting to take place now, it will be a common practice in a few years. A logical consequence of this evolution will be to use IP to access these networks. Figure 6 illustrates this scenario.

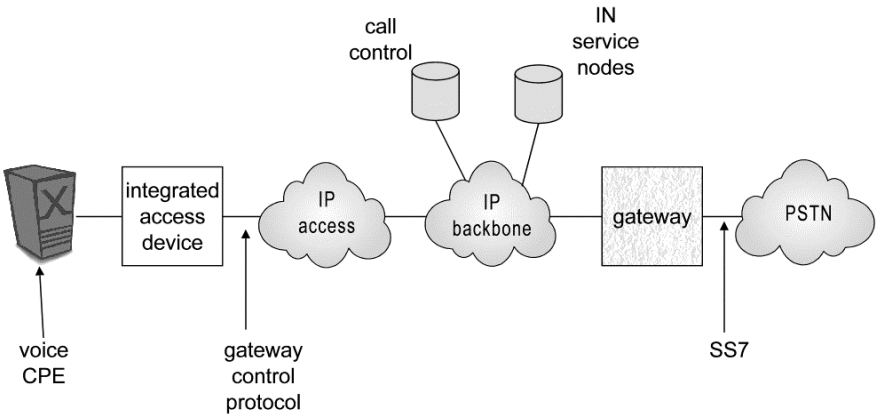

Figure 6 - evolution to SS7

The approach adopted by Inalp Networks of using IADs linked to IP access networks makes this evolutionary path feasible by supporting feature tunnelling in the ISoIP protocol and the V5.2 scenario. Starting from this point of a fully supported interface to a legacy system, it is then possible to migrate seamlessly to the SS7 scenario. We have already successfully tested our IADs working with gateways from other suppliers in this situation.

4.3 Providing PBX networking services

Decisions on whether or not to install a PBX network have, up to now, largely been based on factors such as the variable costs of calls between sites over the PSTN, the whole-life costs of the network equipment needed and the costs of leased lines. The additional features given by a PBX network have also played a part in these calculations, but the over-riding factor has been the cost of providing basic voice connections.

In recent years the benefits of data networking services (web, e-mail, LAN services) have led to the installation of IP networks which, in many companies, already exceed the PBX infrastructure in performance and capacity. The communications manager can now rethink the PBX network strategy based on this evolution.

While Frame Relay or ATM based multi-service networks have been an option for large corporations for some time, the possibility of integrating voice and data on IP now enables the creation of cost-effective virtual PBX networks in situations where a conventional PBX network would not previously have been viable.

Figure 7 illustrates in a simplified form how this decision-making changes as converged and virtual PBX networks are considered. The amount of traffic (ie call minutes) passing through the PSTN has to be high enough for the (variable) cost of that traffic to be greater than the fixed cost of providing a PBX network, if the provision of that PBX network is to be justified. Since the fixed cost of converged and virtual PBX networks is lower than that of conventional leased line PBX networks, this break even point is significantly lowered.

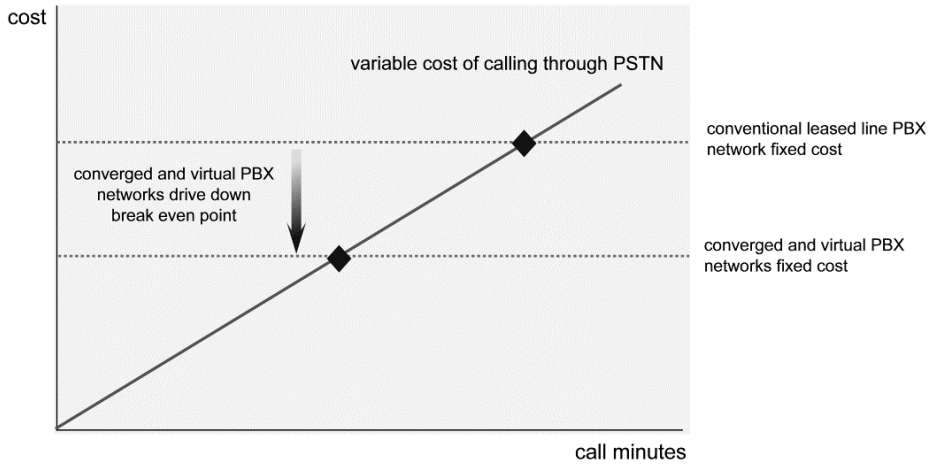

Figure 7 - PBX network costs

4.3.1 Replacing existing networks

Where a conventional PBX network is already in place, the convergence of this network onto the IP infrastructure can cut the costs of using a dedicated leased line and open up opportunities for new IP based messaging and remote access services. The key to making this converged approach a real opportunity is the maintenance of the voice quality and features expected by the users. Since conventional PBX networks rely on dedicated signalling protocols, the support of these protocols is an essential enabling feature in this application.

The Inalp Networks SmartNode products provide Q-SIG tunnelling between the PBXs to support private network features such as private numbering or call-back. Superior voice quality is enabled by the real time IP routing core we provide. By using this approach, features and quality equivalent to the original PBX network can be provided at lower cost. The use of standard H.323 protocols also enables the integration of further value added services on the enterprise network. The interoperability with third

party gateways, gatekeepers and related applications such as messaging services that this approach enables opens a whole range of possibilities. Figure 8 illustrates such a network set-up.

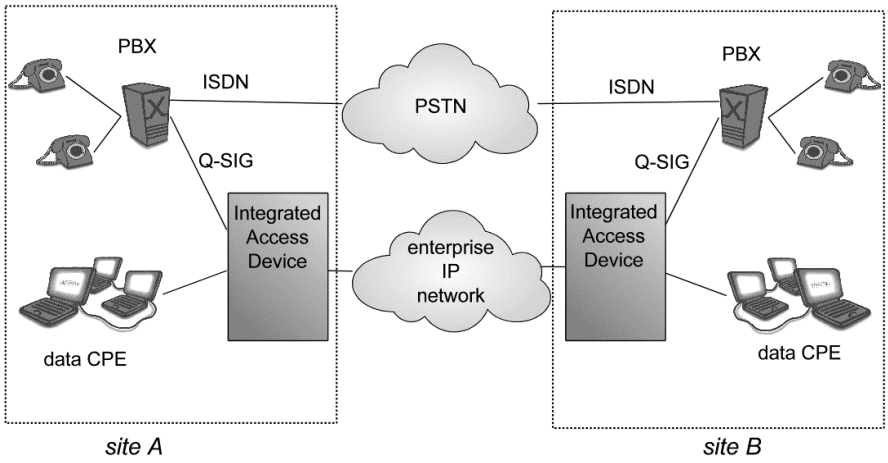

Figure 8 - replacing an existing PBX network

4.3.2 A new network for SMEs without an existing PBX network

PBX networks have not generally been an economic proposition for SMEs with a number of sites. The use of intelligent IADs means that it is now possible to construct a viable PBX network for these SMEs. The IAD provides sophisticated call routing functions and a local breakout path to the PSTN and this makes it possible to use it as the basis for a cost-effective PBX network. Dialled numbers belonging to an enterprise site can be intercepted and routed over the enterprise network while incoming calls and external destinations are routed from and to the PSTN. This results in a "virtual PBX network", without all of the management and equipment overheads of creating a physical PBX network..

The viability of this is further enhanced by the fact that no new interfaces are needed on the customers' premises equipment and no reconfiguration of the PBX is necessary. Figure 9 shows this scenario. This approach is also particularly useful for small branch sites or networks which do not have networking capable PBXs (for example, no Q-SIG support).

This is an attractive option for both the service provider and the customer since it provides a PBX network without the major costs and planning normally needed and allows the network to be reconfigured simply by remotely changing the parameters in the IADs.

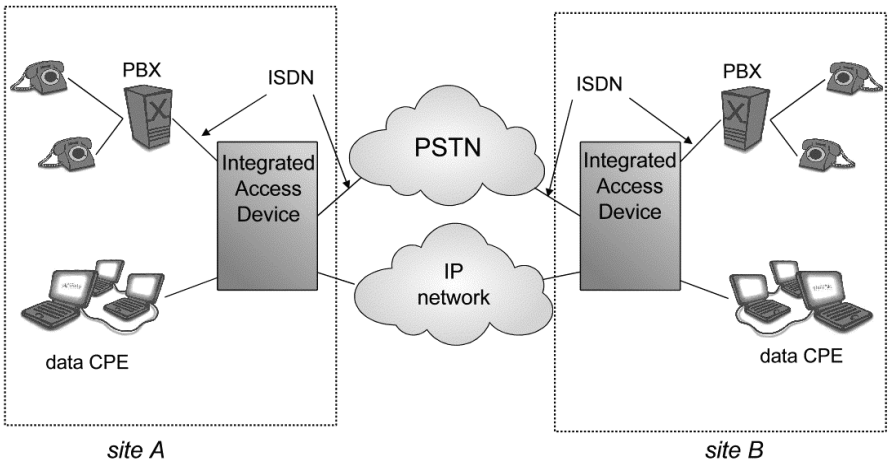

Figure 9 - a PBX network for an SME

4.4 Providing internet access to business customers

SOHO routers are now becoming sophisticated enough to take a major share of the access market for small enterprises. They can benefit from the high volume infrastructure which has primarily been put in place for the residential market – such as DSL, cable TV and dial-up. However, in looking at the options for providing access for small businesses, it is important to bear in mind that there are fundamental differences between the needs of residential users and those of small businesses.

Perhaps the main requirement that distinguishes a small business user from a residential user is the necessity to share the internet access between multiple workstations on a LAN. Another important factor to be considered is the increased security requirements of a business. These strongly influence the features that must be provided by the access device.

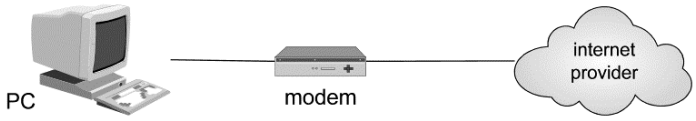

Figure 10 - a typical residential set-up

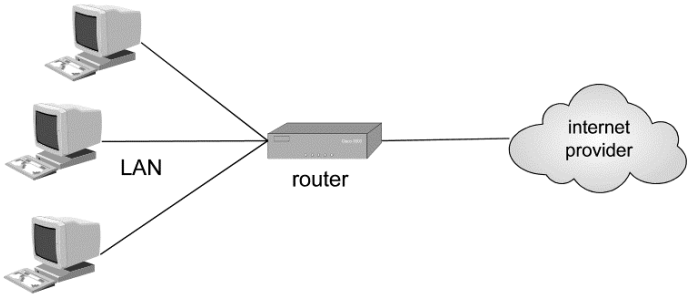

Figure 11 - a typical small business set-up

4.4.1 Addressing

The connection of several workstations on a LAN to the internet creates a number of addressing issues which have to be handled by the access device – such as Network Address Translation (NAT).

In theory, it is possible for a fixed publicly visible IP address to be allocated to every workstation. However, that would be expensive, cumbersome and very wasteful of IP addresses. It would also pose security risks by making individual workstations more visible to the outside world. Instead NAT is used to provide a degree of isolation between the addresses which are publicly visible and the addresses used within the LAN to identify workstations, while at the same time ensuring that data is routed correctly between workstations and the internet

Inalp Networks' approach to solving the addressing problems is to use an IAD to supply the functions which are needed to share internet access. For example, the IAD provides network address translation, acts as a DHCP server for the LAN hosts (eg the workstations), and provides DHCP and PPP clients for provider access.

4.4.2 Security

Another concern for all businesses who have to connect their internal networks to external networks is that of security.

Network address translation (NAT) already provides a high level of security by effectively making the internal structure of the customer's network (eg IP addresses) invisible to the outside world. In addition

to this, the Inalp Networks IAD helps to protect the SME by providing packet filtering security functions to limit access from the internet to the LAN. However, it is important to remember that, while the facilities provided by IADs create a major addition to the armoury of security measures available to the business, they do not replace all of the existing measures. Thus, for instance, it is still important to use good anti-virus software within the internal network.

4.5 Providing virtual private network services

Virtual Private Networks (VPNs) allow companies to connect their sites by using the public network to create their own "private" network, without the expense and inflexibility of building their own physical network. If VPNs are to truly emulate physical private networks, they have to provide the same level of guaranteed throughput and security. There are a number of features which enable this to be achieved on integrated networks.

4.5.1 Provider initiated Virtual Private Networks

The most obvious approach is for the customer to initiate the VPN by creating VPN tunnels through the provider network between the customer's sites. This approach is shown in Figure 12. Connection between the customer's sites is achieved by using this VPN, via the provider's network, and connection to the internet is also through the provider's network, with a firewall being maintained at each site which has internet access.

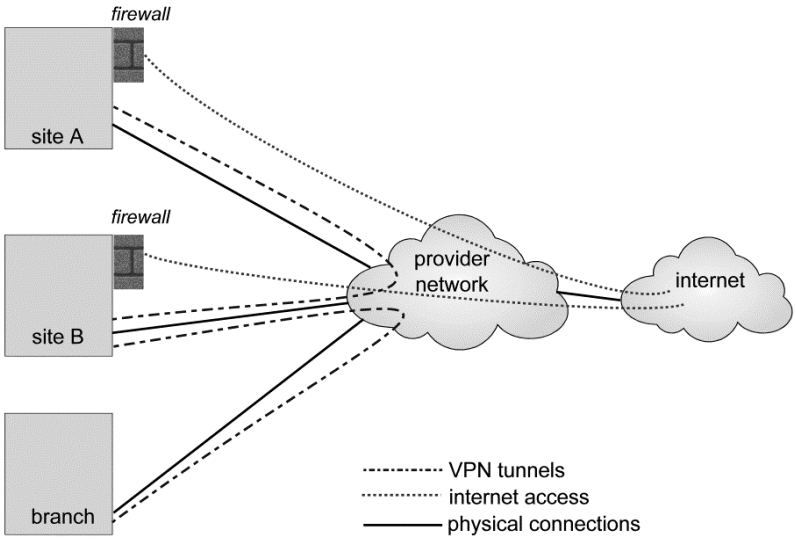

Figure 12 - customer initiated VPN

A more effective approach is for the service provider to initiate a VPN tunnel at his access concentration point (Point of Presence) rather than on the customer's premises equipment, and to support multiple permanent virtual circuits for the customer. This approach frees resources (and reduces cost) on the access router at the customers premises and makes the VPN more flexible, since new sites can be added by the service provider without reconfiguration of the routers at each of the existing sites. This approach is shown in Figure 13.

In the provider initiated VPN, the use of frame relay allows the combination of VPN traffic and internet traffic on the access link. This means that the access router must separate the traffic onto two different PVCs which are then routed accordingly. This solution has the additional benefit of freeing bandwidth on the access link which would otherwise be used by the overhead of routing traffic through a VPN tunnel from each site. Figure 14 illustrates the effects of saving this tunnelling overhead. It must be noted that both the IP overhead and the VPN tunnelling overhead will vary, depending on the mix of traffic.

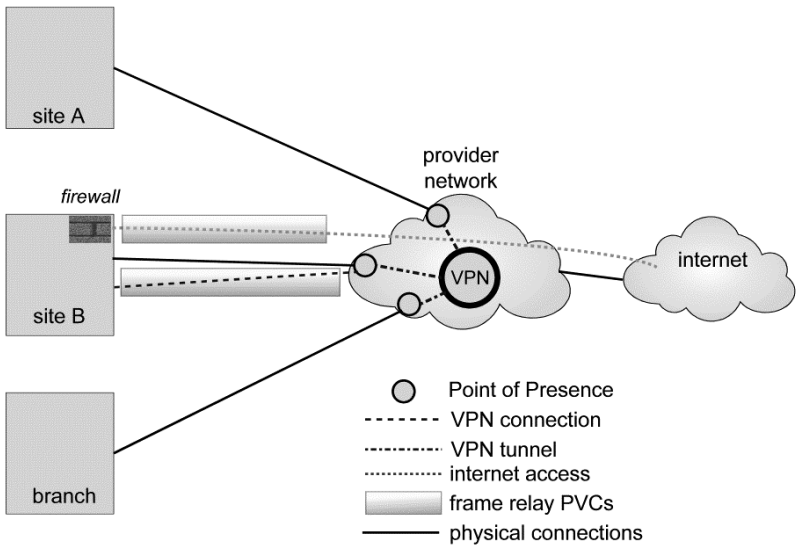

Figure 13 - provider initiated VPN

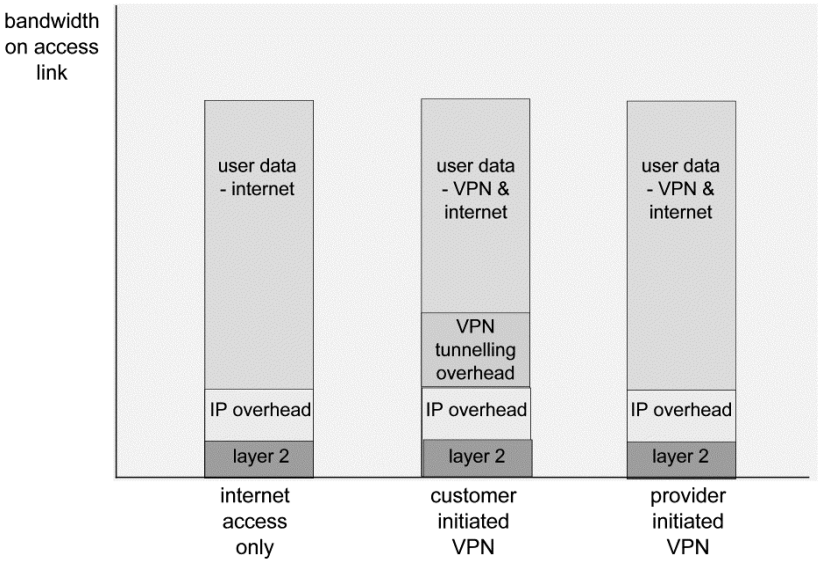

Figure 14 - user data bandwidth

The Inalp Networks IAD makes this approach possible by supporting classification of the traffic intended for the VPN (eg to distinguish between voice and data) and the corresponding prioritisation in the way that the traffic is handled.

4.5.2 Hosted firewall services

Security is a great concern for businesses, especially for SMEs who lack the in-house resources to continuously track potential threats and to update their security measures. Service providers can fill this gap by providing managed or hosted firewall services between a VPN and the internet (see Figure 15). This considerably reduces the maintenance effort needed for updating security measures. It also ensures that there is only a single point of entry and removes consistency and synchronisation problems. It is obviously only possible to take this approach if a provider initiated VPN is used, but it is a major potential benefit of adopting provider initiated VPNs. The way that Inalp Networks IADs support provider initiated VPNs is described on page 14.

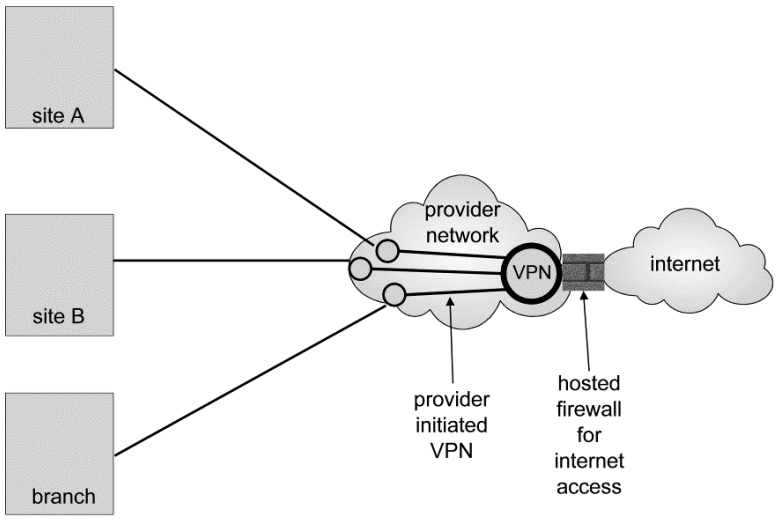

Figure 15 - hosted firewall

4.5.3 CPE initiated support for encrypted tunnels

If the access network is not inherently secure, eg an IP network, then the service provider has to ensure that a method of ensuring the security needed by a VPN can be introduced. The primary need is to make sure that communications within the VPN cannot be tampered with by any outside party. One approach to this is to provide encrypted tunnels within the VPN from the CPE.

The Inalp Networks IAD can be used to support tunnelling protocols and encryption to ensure that a customer's communications cannot inadvertently (or maliciously) be accessed by another person.

4.5.4 Throughput expectations

A key feature of a VPN is that it will carry different types of traffic (eg voice, data, video) and that the customer will expect a defined level of service in terms of throughput for each category of this mixed traffic. This can be difficult to achieve unless a means of differentiating between different types of traffic exists at the point where it is introduced to the service provider's network. It is also important to ensure that any access device does not itself degrade the level of service provided to the traffic.

By adopting Inalp Networks' IADs, a real-time core is provided to make sure that time-critical traffic (eg voice) is not delayed. The IAD can also classify the different types of VPN traffic and provide the necessary prioritisation to ensure that each receives the level of service (eg delay) that it needs.

4.6 Supporting Application Service Provisioning

Application Service Provisioning (ASP) is an important new service. For a number of years, companies have had the problem of supporting a growing number of large, increasingly complex software applications which are essential to their business. With the improvements in communications, it is now possible for Application Service Providers to host these applications, giving the end-user the access they need in real-time but taking the maintenance responsibilities away from the customer.

Obviously, one of the prime requirements of such a service is the reaction time, since the service should behave as if it was locally based. This, in turn, places strict requirements on the behaviour of an integrated network which supports ASPs. The ability of Inalp Networks IADs to classify and prioritise different service classes makes them well suited for use in this application, since the ASP traffic can be granted the priority which it needs to guarantee the reaction times.

4.7 Supporting remote access and teleworking

Recent years have seen a significant growth in the number of employees teleworking and needing remote access to a company's central servers. There are a number of requirements to enable teleworking to be successful, but the chief ones related to communications are throughput and security.

IADs produced by Inalp Networks are particularly well-suited to teleworking, since they are able to provide IP-based communication over the different forms of physical connection (eg cable TV, DSL etc) likely to be found where remote employees are located. Even though they are adaptable to different forms of connection, the features provided by the IADs have a common core and they are managed in the same way regardless of the network technology being used. This common appearance is vital for use within any corporate environment.

4.7.1 Response time

In effect, the need is to extend the VPN out to the remote employee. This means that the features of the IAD which are important for VPNs are also important in this application. A critical aspect is the management of the response time, since the teleworker will be generating a variety of types of traffic and will need to have response times which are within limits set by the service level agreement for the VPN.

As already described, the Inalp Networks IAD can classify different types of traffic and prioritise the way they are handled. This means that the response time for the time-critical traffic (eg voice) can be guaranteed.

4.7.2 PC network transparency

Teleworkers need to have equipment which behaves in much the same way as if they were based on one of the company's main sites, and companies do not want to have to provide individually tailored environments for each teleworker. This means that the IAD and the access need to be compliant with the industry standard solutions for remote access and teleworking. A prime example is that the communications link must be transparent to the Win2000 VPN client.

The Inalp Networks solution is to ensure that the IAD can support PC based VPN tunnel traffic on the NAT and the firewall, in effect providing a transparent link for this traffic.

4.8 Integrating services

This paper has briefly discussed a range of different services and how their needs can be met by Integrated Access Devices fronting an IP-based access network. However, the major advantage of any such network is not its ability to handle individual services, but its ability to handle a mix of services and to flexibly vary that mix.

For this integration to be successful, the service provider has to be able to handle multiple traffic classes and provide (and monitor) the corresponding Service Level Agreements.

4.8.1 SLAs and classification and scheduling

To be able to offer service specific SLAs it is necessary to provide intelligent sharing of the bandwidth available in the network, so that some services can be given a higher priority. Figure 16 illustrates how multiple traffic classes can share the available bandwidth of an access link.

Inalp Networks IADs provide traffic classification that maps customer traffic into priority classes based on layer 3 and 4 criteria. The scheduling then ensures that the prioritisation and bandwidth allocation for these classes is in accordance with the SLA. Figure 17 shows a simplified view of the process of classification and scheduling.

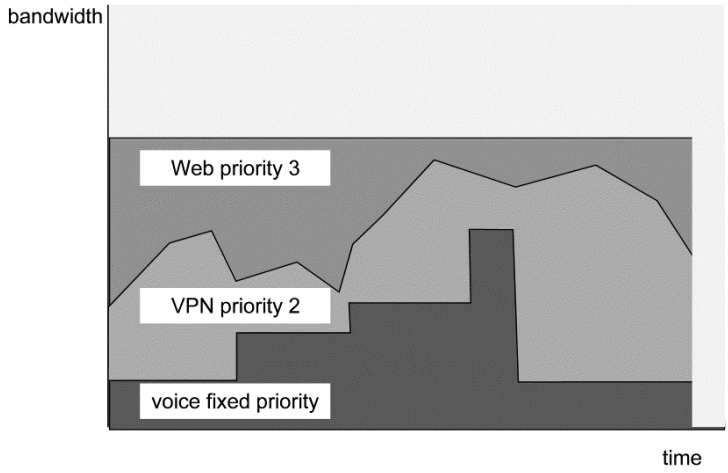

Figure 16 - intelligent use of bandwidth

The system contains two types of queue - the Fixed Priority (FP) queue and Weighted Fair Queue (WFQ). The fixed priority queue serves voice (and other time-critical) services and the weighted fair queue serves the LAN and any other services which are less sensitive to delay. The FP scheduler ensures that the FP queue is served until it is empty. It then allows the WFQ scheduler to serve its queues until another packet is detected in the FP queue. This is an extremely effective way of supporting the jitter and latency requirements of interactive voice traffic.

However effective this process may be, it is not sufficient just to ensure compliance in the access network alone. The IADs also help to ensure that traffic is given the right priority elsewhere in the network by providing network policy compliant labelling of packets (eg TOS, DiffServ) to complement the priority they have been accorded within the IAD.

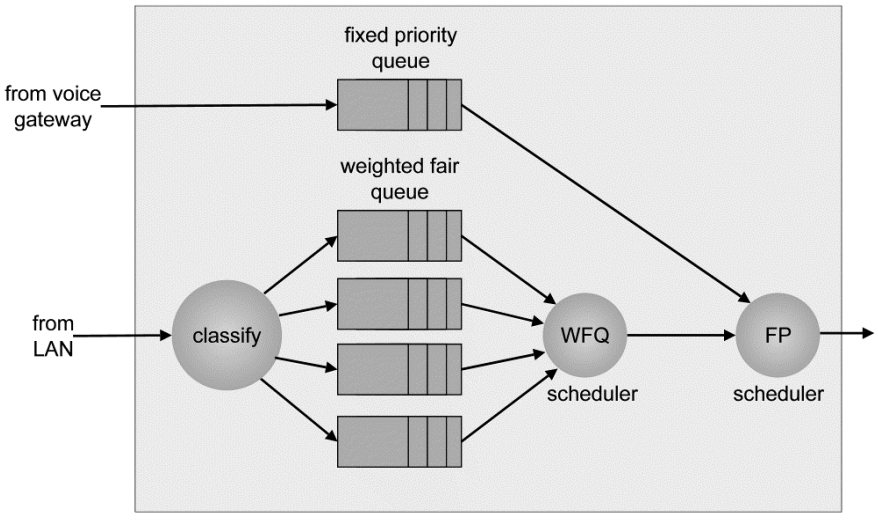

Figure 17 - classification and scheduling

5 Conclusion

Emerging broadband access technologies are opening up new opportunities for service providers. However, just offering the same service ever faster and cheaper is a business strategy which will lead nowhere. To really benefit from the opportunities, service providers need to offer more value to their subscribers. Businesses around Europe are looking for ways to make their operations, communications and workflow easier and more efficient. Value added service providers can fulfil these needs with ready made service packages.

Inalp Networks has put a lot of thought into how these services can be delivered to the customer, because access is a key factor to the success and quality of the service. With this paper we have shown some of the pitfalls that a provider may face and how our products can support him to safely overcome them. The SmartNode Integrated IP Access Devices combine features found in enterprise routers with toll quality voice over IP and a focus towards scaleable deployment and operation. At Inalp Networks we are committed to building access products that can cope with the changing world of integrated service provisioning. 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

ASP Application Service Provider – a provider of software services which can be accessed in real-time by a customer.

ATM Asynchronous Transfer Mode.

CaTV Cable TV.

CLI Calling Line Identity.

CPE Customers' Premises Equipment.

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.

Frame Relay A packet-switching protocol for connecting devices on a Wide Area Network (WAN).

H.323 An umbrella recommendation from the International Telecommunications Union that sets standards for multimedia communications.

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.

LAN Local Area Network – normally used for carrying data around a site.

MPLS Multi Protocol Label Switching - a means of prioritising different types of traffic in an IP network.

NAT Network Address Translator - a device used to extend the internet addresses already in use.

PBX Private Branch Exchange – used for switching voice calls within a company's private network.

POTS Plain Ordinary Telephone Service – the public voice service which we all use on a daily basis.

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

PSTN Public Switched Telephony Network.

Q-SIG A signalling system designed for controlling private networks which carry an integrated set of services. It is compatible with ISDN.

SLA Service Level Agreement.

SME Small to Medium Enterprise – typically a company of anything up to about 100 employees.

SOHO Small Office Home Office – an office based either in the home or containing very few people.

SS7 Signalling System number 7.

TOS Type Of Service information carried in an IP header.

V5.2 The V5.2 standard specifies an open interface for access network systems and was approved by the European Telecommunications Standards Institute and the International Telecommunications Union for PSTN, ISDN and leased lines.

VPN Virtual Private Network - a network that is constructed by using public networks to connect nodes in the private network - for example, using the internet as the medium for transporting data. These systems use encryption and other security mechanisms to ensure that only authorised users can access the network and that the data cannot be intercepted.

WLL Wireless Local Loop – which can replace the fixed (copper) access network and provide broadband access.