

Open-Access Networks

A broadband solution for flexible
business models

TABLE OF CONTENTS

1	EXECUTIVE OVERVIEW	4
2	INTRODUCTION	4
2.1	BACKGROUND	4
2.2	SCOPE OF THIS DOCUMENT	4
3	DEFINING OPEN ACCESS	5
4	POSITIONING PACKETFRONT'S BROADBAND SOLUTION	5
4.1	PURPOSE-BUILT SOLUTIONS FOR THE TRIPLE-PLAY MARKET	5
5	DEFINING THE TECHNICAL REQUIREMENTS OF AN OPEN-ACCESS INFRASTRUCTURE	6
5.1	OVERALL FUNCTIONAL REQUIREMENTS FOR OPEN-ACCESS NETWORKS	6
5.1.1	<i>IP addressing</i>	<i>6</i>
5.1.2	<i>Service deployment and self registration</i>	<i>6</i>
5.1.3	<i>Multi-service deployment</i>	<i>6</i>
5.1.4	<i>Trusting the network</i>	<i>7</i>
5.1.5	<i>Service-provider integration</i>	<i>7</i>
6	CHALLENGES IN AN OPEN-ACCESS INFRASTRUCTURE	7
6.1	ADMINISTRATION	8
6.1.1	<i>The PacketFront response to administration</i>	<i>8</i>
6.2	MASS-DEPLOYMENT TOOLS	8
6.2.1	<i>The PacketFront response to mass-deployment tools</i>	<i>9</i>
6.3	IP ADDRESS ALLOCATION AND USE	9
6.3.1	<i>The PacketFront response to IP address allocation and use</i>	<i>10</i>
6.4	SECURITY	10
6.4.1	<i>The PacketFront response to security</i>	<i>10</i>
6.5	PROTECTION FROM HACKERS AND ABUSE	11
6.5.1	<i>The PacketFront response to protection from hackers and abuse</i>	<i>11</i>
6.6	BANDWIDTH MANAGEMENT AND CONTROL	12
6.6.1	<i>The PacketFront response to bandwidth management and control</i>	<i>12</i>
6.7	TRACEABILITY	12
6.7.1	<i>The PacketFront response to traceability</i>	<i>13</i>
6.8	QUALITY OF SERVICE	13
6.8.1	<i>The PacketFront response to quality of service</i>	<i>13</i>

6.9	BROADCAST DISTRIBUTION	14
6.9.1	<i>The PacketFront response to broadcasting</i>	14
6.10	OPERATIONS AND MAINTENANCE	15
6.10.1	<i>The PacketFront response to operations and maintenance</i>	15
7	CREATING THE NEXT GENERATION OF BUSINESS MODEL	15
7.1	KEY PLAYERS IN THE OPEN-ACCESS WORLD	15
7.1.1	<i>The network owner</i>	16
7.1.2	<i>The service provider</i>	16
7.1.3	<i>The communications operator</i>	16
7.1.4	<i>End user benefits</i>	17
7.2	SOURCING REVENUES	17
8	SUMMARY	18

1 Executive overview

In an environment in which the flexibility to adopt new business models is important, strict requirements are placed on the background technology used in current and future broadband networks. Flexible business models, such as an open-access business model, stimulate revenue-sharing and opens the traditional boundaries between the owner of network infrastructure, the network operator and the service provider.

The open-access business model offers the key players in the distribution chain – end users, network owners, property owners and service providers – tremendous advantages. Each player will be able to focus on its core competencies, assuring timely, cost-effective contributions to the model at all times. The network owners can focus on low-level connectivity, the service providers on competitive services, and the end users will have the ability to choose services on an on-demand basis. One new player is introduced in this model: the communications operator, who holds the administrative responsibility for the overall functionality of the model.

The open-access model requires a new way of thinking from a technological perspective. PacketFront was the first to offer technology that enables the open-access model over IP - IP regardless of physical connectivity to the end user: Ethernet over fibre or copper, VDSL or any other technology that offers the bandwidth required to support triple-play services – data, voice and TV.

PacketFront's experience from designing, building, operating and maintaining the largest Ethernet broadband network in the world places us in a unique position when it comes to understanding how closely the technology is related to the business model, and what ultimately carries a broadband operator from idea to profitability.

2 Introduction

Cost-efficient operation of a broadband network in a triple-play environment poses major challenges. This paper will discuss the challenges and the possibilities that lie within the domain of the construction, operation and maintenance of open-access networks.

2.1 Background

Many clients, from various industries and in various parts of the world, are considering entry into the IP and/or fibre-based broadband market. The utility sector, cities and communities, property owners and cable-TV operators are all looking for new ways to expand their product portfolio, improve public services, increase property values, build the next generation of television distribution networks, or simply find new ways to increase their revenue base. One common issue that all of these players must face is the high technical complexity of the field of IP-based open access.

2.2 Scope of this document

The purpose of this document is to illustrate how technology solves the challenges of open access, and simplifies areas that are often considered to be complex. Furthermore, this document will introduce the players, describe their prime motivations, and present a potential business model.

3 Defining open access

The first key motivation for this kind of network is the ability to handle all three main categories of services – data, voice and TV, also referred to as triple-play services – over one physical infrastructure.

A further motivation is the ability to distribute these services to the end user from multiple service providers. The end users will have the option to choose one type of service from several competing service providers within the same physical infrastructure – in real time.

The most important benefits obtained when using open-access networks include:

- the increase in network traffic that is a result of end users' growing use of broadband services that tend to happen when the service offering is extended.
- the end-user's freedom to choose the service provider that presents the most attractive offer in terms of service quality and cost.
- the ability of the service providers to provision the services over multiple broadband networks independently of the network ownership.
- the positive influence that advanced broadband deployment has on economic development.

PacketFront's definition of open access is:

“An open-access network allows for unlimited integration of 3rd party service providers into a single physical infrastructure, yet maintaining vital functionality such as security, hacker & abuse control, service distribution control, service provider specific IP addressing, protection and quality of service, and finally, provide the ability to control and cut OPEX.”

4 Positioning PacketFront's broadband solution

This section focuses on placing PacketFront's broadband solution into a network view, i.e. explaining where our solution is located in the broadband network.

4.1 Purpose-built solutions for the triple-play market

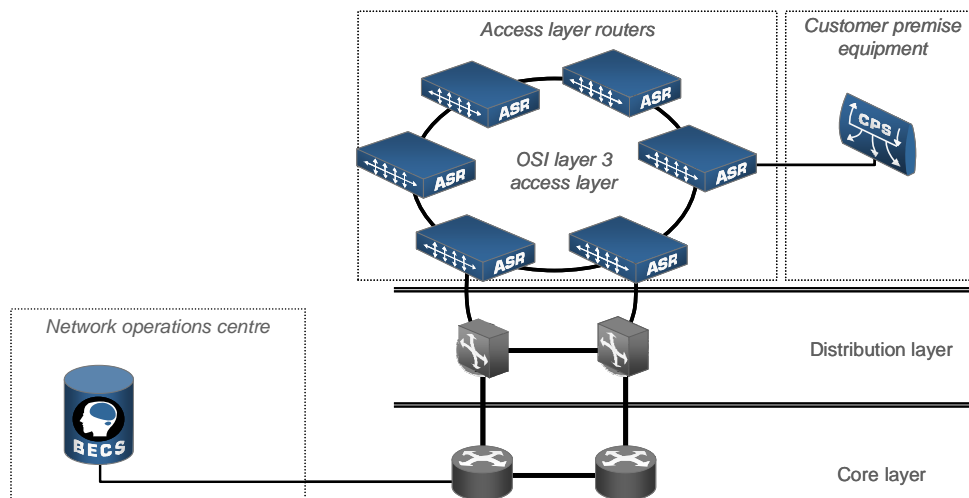
The technical requirements of triple-play and open-access networks create the need for purpose-built solutions that satisfy these requirements. Office-switching equipment cannot meet these requirements.

The objectives of a purpose-built solution include the following:

- to offer maximum flexibility in the creation, differentiation and provisioning of services.
- to enable new business models by allowing multi-service distribution in an open-access infrastructure.
- to focus on keeping the OPEX to a minimum.
- to focus on keeping the CAPEX to a minimum.
- to offer a carrier-class, scalable architecture that solves known technical issues.

With regard to the specific objectives above, PacketFront offers an automated broadband solution that features a broad range of integrated functionalities. The main parts of the solution are:

- BECS™, the control and provisioning system, and
- the ASR series of broadband routers powered by the iBOS software



5 Defining the technical requirements of an open-access infrastructure

PacketFront has defined a set of functionalities that the network must perform in order to comply with the definition of open access. These functionalities are discussed in greater detail below.

5.1 Overall functional requirements for open-access networks

5.1.1 IP addressing

The fundamental capability of an open-access infrastructure is the ability to dynamically allocate a public or private IP address from the IP scope of one or several specific service providers to an end user. It should also be possible to extend the IP address to a specific end-user device (PC, set-top-box, IP telephone, etc.).

5.1.2 Service deployment and self registration

An open-access infrastructure must be capable of handling a virtually unlimited number of services. In the traditional telecommunications model, this is not possible due to enormous development costs and operating costs. In order for an open-access network to work in a credible manner, the network must support a self-registration mechanism in which a device requiring a specific service is registered with the centralised abstraction layer.

5.1.3 Multi-service deployment

Once the user-verification and service-verification processes have been completed, the network must be able to meet the requirements set by the service itself. These requirements may be bandwidth management and latency requirements for IP telephony, bandwidth and multicast access for TV distribution, bandwidth availability for Internet transit bandwidth as opposed to bandwidth allocation for broadband intra-net traffic, etc. Once the quality required has been determined, the network must be capable of dynamically adjusting its configuration parameters, without further involvement from the network operator and/or service-providers' customer support.

5.1.4 Trusting the network

An issue that arises frequently in today's layer 2-based broadband infrastructure, is the problem of IP/MAC address cloning and ARP spoofing. The system must be capable of guaranteeing that only the user that is actually paying for a service is actually using it. Existing solutions based on enterprise office switching equipment do not provide the necessary traceability and identification mechanisms.

The network must be capable of supporting reliable and controlled synchronous routing for Internet services in an open-access infrastructure.

5.1.5 Service-provider integration

The next level of complexity is related to providing third party service providers with the ability to: a) provision their services, b) trust the network to deliver the services that have been agreed upon, c) follow up on the quality of the service distribution, and d) trust the billing records to reflect the actual use of a service. These four abilities are fundamental, but very complex, as they require a tight integration between the network owner and service provider's Operational Support Systems, OSS.

PacketFront's broadband solution is a fully integrated system covering all aspects discussed above.

6 Challenges in an open-access infrastructure

The next sections cover issues related to the mass deployment of multi-service applications in a multi-service-provider-environment. It is important to understand the challenges related to mass deployment. Most services and network platforms will perform adequately in a laboratory environment or in a small-scale pilot scenario, while the true challenges only become apparent during large-scale deployment. All aspects of PacketFront's solution are therefore developed with *scalability* as their leading star.

The main challenges of large-scale deployment will be discussed with respect to:

- Administration
- Mass deployment tools
- IP allocation and utilisation
- Security
- Protection from hackers and abuse
- Bandwidth management and control
- Traceability
- Quality
- Broadcast distribution
- Operations & maintenance

These challenges are all relevant for all types of broadband operators, but they have special significance for the open-access operator, relating to the ability to roll out services in a pre-determined, scalable and controlled manner.

6.1 Administration

A network operator and/or network owner must handle several hundreds of thousands of physical end-user interfaces, hundreds of thousands of end users, multiple & simultaneous services with different network requirements, additional growth of the network, growth in the number of end users, changes in end-user data and the services they subscribe to, and thousands of access layer network nodes.

The only scalable scenario that can cope with this kind of network is the approach to service level management. An abstraction layer is needed and must be capable of dealing with the challenges mentioned above with a minimum involvement of personnel, yet maintaining a low level of erroneous configurations, in order to make these environments manageable.

Existing broadband operators are experiencing a significant challenge in keeping the operating expenditures, OPEX, at a reasonable level. Maintaining OPEX at a low level is vital, due to the nature of mass deployment in a consumer market. Problems arise mainly as a result of poor integration of the network elements, network management systems and the service-provisioning systems. If these systems are not tightly integrated, there will be a large need for manual intervention in the configuration process of the services, slowing the service deployment and making it more prone to error. This will result in high OPEX and lower revenues due to lower customer satisfaction levels.

Most broadband operators currently employ armies of technically competent people responsible for the re-configuration of network elements and other peripheral systems. This is a costly and slow procedure that must be handled by the centralised abstraction layer.

A second key concern is to make sure that the billing system is in level with the service provisioning system of the service provider and the network operator. Experience shows that a great deal of inconsistency can arise between the data records sent and received, the services provisioned and the actual bill being sent out to the subscriber. This creates unnecessary frustration for the customer.

6.1.1 *The PacketFront response to administration*

PacketFront's solution is based on using BECS, the control and provisioning system, in combination with SMT, the Subscriber Management Tool, or by directly integrating other operational support systems to our TIBCO TibRendezvous data bus interface.

BECS provides the abstraction layer that controls the complete infrastructure, its services and its end users. SMT offers the service provider the tools required to register, provision, troubleshoot and event-browse address logging and other incidents.

6.2 Mass-deployment tools

If not implemented carefully, mass deployment tends to consume enormous amounts of resources. The network operator must for this reason be able to deploy and configure new network elements as rapidly and as cost-effectively as possible.

This is currently achieved by the network operator sending out competent installation resources into the field, with the network element under his/her arm, installing it in a rack (or equivalent), and configuring the basic parameters required on site. This has been necessary, since the network node will have different configurations depending on the physical location. Needless to say, this requires competent and highly educated resources.

This kind of initial configuration management tends to slow deployment and increase OPEX to unnecessary levels.

6.2.1 The PacketFront response to mass-deployment tools

The mass-deployment function in BECS is our response to cutting time, reducing errors and minimising OPEX related to initial configuration of network elements.

The complete network topology is pre-configured in the centralised BECS. The IP addressing structure, the physical interface configurations, basic service support, etc., are all handled in a proactive manner. This allows for very efficient network node implementation. The entrepreneur responsible for the installation of the physical cable can also take responsibility for the physical mounting of the network node. Once the network node has been installed and powered, it will boot and request its IP address and configuration files from BECS. BECS will identify the node based on its topology instructions in its database. Once the network node has been identified, the configuration data is downloaded to it, and the end users connected to this node will be up and running, without any form of manual intervention at this initial stage.

This approach reduces the number of trained personnel for initial configuration in the field to zero.

The same process is used if a network element must be replaced due to failure. Once powered up, it will find its place in the topology via BECS and be up and running within minutes – without needing any on-site Internetworking experts.

6.3 IP address allocation and use

IP address allocation and use is a major challenge for all operators in the mass-deployment market. A number of factors must be considered.

Internet currently uses Ipv4, and will do so for the foreseeable future. The address space is allocated by the IANA/RIPE organisation. The IPv4 address space is very limited, and thus addresses allocated must be used as efficiently as possible. IANA/RIPE may restrict addresses allocated to a specific provider who uses the addresses allocated inefficiently.

This is particularly interesting for IANA/RIPE when it comes to consumer networks, due to the sheer number of addresses required. The allocation of public IPv4 addresses is only allowed under certain circumstances, and only one IPv4 address can be allocated per Internet user. (This restriction is not relevant for IPv6.)

Hence, an end user might end up having an IP telephone with a public IPv4 address, a set-top box (STB) for TV distribution and video-on-demand with a private address, and a PC with a public IPv4 address. The complexity is further increased as the various services are offered by different service providers, who all use their own IANA/RIPE registered IP scopes.

6.3.1 The PacketFront response to IP address allocation and use

PacketFront's broadband solution handles all aspects of IP allocation in a multi-service provider environment, as discussed above. The BECS IP-allocation function handles the IP allocation, and the ASR broadband router is capable of handling multiple IP subnets, private and/or public, on the end user line interface.

IP address allocation in BECS is matched with the services the specific end user has registered for a specific device, and complete control of IP address allocation is achieved.

BECS offers another valuable function, known as "IP address over-allocation". This is the capability to overbook end users to the available number of IP addresses in a superior manner. Over-allocation is achieved by using large address pools that are not bound to physical boundaries or to VLANs (virtual local area networks), and dynamically allocating addresses to the routed environment.

6.4 Security

A common issue in triple-play networks has been the lack of control and inter-user security. Maintaining integrity has been a major challenge, and it has often been neglected or solved in complex, non-flexible and non-scalable manners. Negative exposure in the media will automatically result from a failure to offer a certain minimum level of security.

Security must be considered with reference to service transparency. Security and service transparency do not go well together. An operator must implement firewall functionality, i.e. filtering on layer 3-7 of the OSI model, in order to guarantee a certain minimum level of security.

A simple example is the use of Microsoft Networking. This allows end users to access each others' hard drives, printers, etc. This can be a major security risk – especially for end users who are not very technically oriented, and who use Internet for banking, etc. Existing networks are usually able to filter out this protocol, but this will result in an inability to run other Microsoft-based applications. User-specific security levels do not usually exist.

This can quickly become a major headache for the service provider. Consider a household in which the functionality for Microsoft Networking has been disabled. A housing facility or landlord might want to base their booking system for the laundry-room on the system, or they may want to share the minutes from committee meetings of the housing facility with residents. This cannot be done without allowing the end users to remove security filters. Furthermore, an end user who wants extended security might want to add extensions that allow only E-mail and web surfing. This requires advanced user-defined capabilities.

The network must therefore allow security limitations to be defined with a much higher degree of granularity and user orientation than the degree that is possible in existing broadband infrastructures.

6.4.1 The PacketFront response to security

One way to handle security is to offer differentiated security services, where filtering capabilities are implemented on a user-by-user and device-by-device basis. This will satisfy the various end user needs, and it will create a basis for further revenue generation. It will also prevent negative media exposure.

PacketFront's broadband solution is based on layer 3 routers in the access layer, and the use of PPP, L2TP and similar tunnelling protocols can therefore be avoided. These solutions do not scale and they require (in most cases) a software client in the end-user PC. Mass deployment using solutions of this nature will drive OPEX to new heights.

As described in previous chapters, BECS maintains control by correlating information such as DHCP vendor field information, IP address, MAC address, network node interface and network node ID. This information is then used for downloading dynamic configuration data to the specific network node.

The security aspects are another set of configuration parameters that can be dynamically downloaded to the network node. Services can be created and subscribed to by the end user through the self-registration interface. Hence, the end user can subscribe to a specific security service relating to his/her needs and competencies – without the involvement of network operator staff.

The filters implemented by BECS operate on layer 3-7 of the OSI model, making it possible to achieve total granularity in any security service.

The security features can be implemented on a service-by-service basis. This allows the open-access environment to remain uninterrupted, and it provides the service provider with a guarantee of service transparency as defined by him/her.

6.5 Protection from hackers and abuse

Hacker attacks and other abuse are serious issues in today's broadband networks. Any user with an always-on connection will be exposed to hacker attacks and other abuse. Providing some level of security is the first step as discussed in earlier sections.

Network-level attacks pose a more serious problem. These attacks are directed at the network itself, with the aim of disrupting operations, disrupting services, stealing an end user's identity, or even faking the absence of a router, which forces all traffic to be directed to a specific machine and not to the network elements that are its intended target.

All these attacks directly affect customer satisfaction, OPEX and revenue potential. It will require extensive effort to reinitiate a service that has been disabled after abuse, and the problem may very well reoccur, if the protection is insufficient.

Furthermore, an unstable service will not generate revenue at the pace defined in the business case. Unstable services will make the open-access infrastructure uninteresting – both to the end user and the service provider, and an open-access infrastructure without services is a “dead” proposition.

6.5.1 The PacketFront response to protection from hackers and abuse

BECS maintains control by associating information such as DHCP vendor field information, IP address, MAC address, network node interface ID and network node ID with the services to which the end user has subscribed. This information is translated into configuration files for the network elements. Combined with its advanced routing mechanisms, the PacketFront solution prevents:

- ARP cache flooding
- ARP spoofing

- Multicast head-of-line blocking and service disruption
- MAC address cloning
- IP address cloning
- Layer 2 security holes

Prevention of these attacks is required in order to provide the user with a secure and reliable mechanism for multi-service distribution in a multi service-provider environment.

6.6 Bandwidth management and control

A major concern for broadband operators today is controlling the bandwidth allocated and used at the levels of end user, service and household. Multiple simultaneous streams of several services must be controlled, identified and managed.

The network operator/owner must be able to set rules that differentiate between the usage of bandwidth in certain steps and degrees. It must be possible to differentiate the bandwidth and to relate this to the services. One end-user unit might require 13 Mbps for his/her TV service, while the Internet bandwidth availability is to be set to 256 kbps, and the available local broadband network bandwidth may be limited to 10 Mbps.

This is a rather unexplored area, and service providers and network operators around the world are looking for this possibility since it provides an operator with several important functions of running an open-access network.

6.6.1 *The PacketFront response to bandwidth management and control*

PacketFront's solution can provide bandwidth allocation on a per service/device level in steps of 64 kbps – in a centrally managed, dynamically configured and controlled manner.

The ability to control the bandwidth allocation makes it possible to differentiate services. This provides added value, and it provides bandwidth cost control and a significant source of revenue for the network operator.

The ability to control the bandwidth allocation also makes it possible for the Internet service provider to sell a managed Internet connection with limited bandwidth. Bandwidth abuse over an Internet connection is a major concern. Transit costs are escalating out of control, due to consumer behaviour in broadband networks.

6.7 Traceability

A key concern for an operator is the ability to track and trace the end users of the network. Scalable, reliable and secure ways of tracing an end user are not currently available for broadband networks. It is fairly easy to steal a MAC address or an IP address. The methods currently used to deal with such theft include PPTP, L2TP, etc., which are all server-based solutions that provide little or no reduction in OPEX, and poor scalability, availability and performance.

For the sake of scalability, it is vital that the traceability features implemented do not require the installation of client software at the end-user. Nor should an end user be forced to log in with username and password every time he/she wishes to use a service.

6.7.1 *The PacketFront response to traceability*

BECS maintains a database in which every IP address used in the network is mapped to the corresponding MAC address, service selected, connected port and router, together with a billing ID and a timestamp.

This allows the network operator and service provider complete traceability of the end users throughout the network.

6.8 Quality of service

The ability to ensure a certain quality of service, QoS, is the key to success for an open-access operator. It is extremely unlikely that a service provider will operate in a shared environment unless QoS is guaranteed.

QoS is particularly important when the network load peaks at the limits of available bandwidth, or when the network experiences a link down or a network node failure. The failure conditions will force traffic to take alternative routes – routes that may already be on the verge of congestion.

Applications such as IP telephony and video conferencing are interactive real-time applications that must be given absolute priority in the network, end-to-end. Other applications are less time-sensitive, but still require a guaranteed bandwidth. These include TV distribution and video-on-demand.

The network must be able to differentiate between these services and to guarantee the requirements posed by a specific service. This poses yet another challenge.

Once the network is capable of assigning different priorities to traffic and guaranteeing bandwidth and latency, malicious users will start to attack this by setting their own priority to *High*, thus claiming an unfair amount of prioritised bandwidth in the network.

6.8.1 *The PacketFront response to quality of service*

PacketFront's solution addresses these issues using the concept of "trusted" and "un-trusted" traffic. The network reacts to trusted traffic by giving the QoS that a specific IP packet or data stream from an end user requests.

The network reacts differently to un-trusted traffic. Traffic entering the network is always considered to be un-trusted. The network elements always take actions to verify the IP packets and traffic streams by re-labelling the TOS (Type Of Service) field in each individual IP packet. The traffic is re-classified to match the priority level that has been defined in the dynamically allocated BECS profile.

QoS management is handled in a policy-based way, by the service definition and distribution settings in BECS. BECS functions as the policy decision management server, while the ASR broadband routers are the policy enforcement nodes in the network.

The ASR broadband router can deal with multiple HW queues for each physical interface independently configured in two directions, and managed by advanced congestion management algorithms. All QoS rules are implemented dynamically at full wire speed. The QoS features of the system do not degrade performance at all.

6.9 Broadcast distribution

The distribution of services such as TV, radio, near video-on-demand, etc. requires the network to provide specific mechanisms that are capable of selective broadcast. This ensures that only those end users, who have subscribed to a particular broadcast service, are capable of using this particular service.

This is implemented through the mechanisms of “IP multicast”. Multicast is a form for selective broadcast, where the client can receive multicast streams only if he/she has subscribed to the specific multicast channel.

Service disruption and channel swapping times are important issues that must be considered when using multicasting in IP-based networks. The first issue has been discussed earlier in this document. Rapid channel swapping requires an optimised solution that allows the network to close down one multicast stream rapidly for the benefit of another.

6.9.1 *The PacketFront response to broadcasting*

PacketFront’s solution is based on using layer 3 broadband routers in the access layer. Multicasting, QoS and other topics discussed in this document all operate on layer 3 and 4, the same layer as the router.

This means that the multicasting implementation can be highly optimised. The result is a very fast multicast network with the ability to converge (recover after network failures) in a very short time.

The solution allows for a single end-user unit to subscribe to several multicast groups/streams at the same time, and it exploits the QoS mechanism discussed in the previous chapter.

The channel swapping times of PacketFront’s solution are as low as 200-300 milliseconds. This is shorter than the MPEG-2 synchronization time specified by the MPEG-2 standard, and this means that changing a channel is not experienced as a time-consuming procedure.

The solution also offers conditional access for the multicast services provisioned in the network. BECS will check the database in order to verify which multicast groups the end user and/or a specific device is allowed to receive. Once this is established, BECS will dynamically update the network with the appropriate information relating to the distribution of the multicast streams.

This mechanism breaks new ground in using IP as a technology for TV distribution. The network now controls the conditional access system, and no TV channels can be viewed without the authorization of the BECS system. In existing TV networks this decision is usually left to the SmartCard implemented in the TV decoder.

The SmartCard cloning market is huge and creates large holes in the pockets of the content-owners, denying them of considerable revenue. PacketFront’s solution makes SmartCards a thing of the past, and provides a secure and future-proof platform on which TV distribution can move ahead.

6.10 Operations and maintenance

An open-access operator requires maximum uptime. The system must have a very high MTBF, mean time between failures. Furthermore, it is imperative that the network elements can sustain the lifecycle required by the business case.

A common problem in today's networks is the environment in which the network elements are placed. A humid, dusty and warm environment is not a suitable location for office switches. Analysis shows that as many as 6-8% of all switches installed suffer from problems related to dust and moisture so severe that the node must be replaced.

Experience shows that currently the most serious problem in broadband networks relating to HW faults is the fans and power supplies. Vendors, however, continue to deliver integrated elements, and the whole switch must be replaced when any of these components fail.

6.10.1 The PacketFront response to operations and maintenance

PacketFront's solution is purpose-built for the environment in which it is to be placed. This means that the ASR broadband router is free from fans and other forms of mechanical cooling. The power supplies are external and available in redundant design.

The ASR broadband routers have been designed for service provider environments and they have been thoroughly tested for blows and drops.

The network design proposed by PacketFront is fully redundant and self-healing in the event of line or unit failure. The design is based on layer 3 routing, and this means that convergence times are minimized – which is not the case in layer 2 networks.

The ASR broadband router will automatically reboot after a power failure, retrieve the configuration information and be fully operational within 60 seconds.

7 Creating the next generation of business model

Open-access networks promise the ability for multiple players to get together and share the investment required to build the next generation of communication networks and services. This sharing of investment leads to a revenue-sharing model in which all parties receive their fair share of the income generated from services – weighted to take into consideration the risk experienced and the investment made by each contributor.

Lowering the barriers to entry is the key promise of an infrastructure that is able to provide open-access networks, and that is the main attraction for service providers, network operators and end users.

7.1 Key players in the open-access world

We introduce three players – the network owner (NO), the communications operator (CO), and the service provider (SP).

It is vital that all of these players have clearly defined areas of responsibility, since the open access infrastructure distinguishes clearly between them.

7.1.1 *The network owner*

In the open-access model, each type of network owner is specialized within a certain field. For the purpose of simplicity, we have let the network owner be represented by:

- The property owner
- The city network owner
- The backbone network owner

Each of these network owners faces different challenges when using the old telecom model.

The property owner is concerned about the freedom of service selection for his/her tenants, the various types of infrastructure required for service distribution in the building, and the financial net result of the infrastructure.

With the open-access model, the value of the property will increase, the tenant is offered freedom of choice in service selection, one physical infrastructure is carrying all services, and a more viable economical solution is given.

The city network owner must consider the existing pricing model and structure, the selection of services available in the network, placement in the value chain, and the economies related to growing the network.

The open-access model offers the city network owner: the ability to focus on core business – the network and the ability to increase the number of services offered – thus increasing the attractiveness of the network offering and increasing the revenue base, and finally the ability to grow the network in a foreseeable and financially controllable manner.

The backbone network owner is mainly concerned with spare capacity and how to increase the customer base.

The open-access model provides the traffic required to fill the spare capacity of the backbone provider.

In the open-access model the network owner focuses on the ability to provide a physical connection to the end user. Revenues from services will emerge from third parties through the revenue-sharing model with minimum investment in service development.

7.1.2 *The service provider*

The service provider's main concern when using the old telecom model is what kind of network to use and how to increase its customer base without major upfront investment. Many service providers are forced into network deployment with very few customers, and they are for this reason forced to look at profitability from a long-term perspective.

Economies of scale can generally be applied to a service provider, and obtaining access to a wide customer base is for this reason of great interest.

In the open-access model, the focus of the service provider is his/her ability to create cost-efficient and competitive services – without considering the network aspects.

7.1.3 *The communications operator*

The communications operator is a new element introduced into the open-access model, with the following key areas of focus:

- the ability to enable the network owner to increase the network offering within reasonable economical boundaries.
- the ability to minimise the needs for initial investment by the service provider, and to increase the availability of services offered to the subscribers.
- the responsibility for the establishment of a balanced revenue-sharing model between all the involved parties. The commission for the lower level infrastructure must be in line with the number of end users on the network and with service development.

The communications operator will thus act as the administrative entity ensuring that all interfaces are implemented in a reliable manner.

7.1.4 End user benefits

The old telecom model locks the end user rigidly into the service offered by the owner of the physical infrastructure. This applies to incumbents, cable TV operators, phone companies, etc.

With an open-access model in place, there is no relation between the network owner and the services offered. All that is required is a network capable of dealing with the aspects discussed in chapter 5 of this paper.

The end-user will be able to choose from multiple services in a competitive environment, ensuring that quality and costs are optimised.

7.2 Sourcing revenues

The key to the business model lies in the revenue-sharing aspects and in the distribution of responsibility for creating the vital sub-systems that make up an infrastructure capable of supporting an open-access network.

The revenue-sharing process can be implemented in the following way:

1. The communications operator provisions the services in the network through its service gateway.
2. The end user self-registers for a service.
3. The service is distributed from the service provider, via the communications operator, to the end user.
4. The service provider bills the end user directly.
5. The end user provides a kick-back to the communications operator.
6. The communications operator provides a kick-back to all network owners.

8 Summary

This paper discusses the requirements of an infrastructure capable of offering an open-access network. In order to reach a viable broadband network, the solution must be handled as one integrated system. It is not possible to implement the boxes first, leaving management, control and provisioning to be dealt with later.

- The solution must be capable of integrating an unlimited number of services from an equally unlimited number of service providers in a scalable manner.
- The solution must be capable of provisioning data, voice and TV services.
- The solution must be capable of guaranteeing no unauthorised use of services.
- The system must provide the end user with a self-registration interface.
- The system must efficiently handle IP addresses provided by the service providers.
- The system must be capable of handling a mix of public and private addresses within the same household.
- The system must be capable of integrating with the service providers' provisioning system in a scalable and efficient manner.
- The system must provide interfaces based on open standards for third party OSS/BSS integrations.

A system that cannot provide all of these functions cannot claim to provide an infrastructure that is capable of open access.

It is PacketFront's strong belief that the telecommunications market is facing the opportunity to pick up the pace again, and that a completely new approach to how business is created and how costs and revenues are shared amongst the contributors in the overall model is necessary.

In the near future, we will see a wide variety of implementations of these new business models, but the basics will remain the same.

- The network owner will provide physical connectivity.
- The service provider will offer services.
- The communications operator will be the administrative entity that co-ordinates the complete enterprise.
- The end user will be the winner, with a wide variety of services offered at low cost and at high quality.