TECHNOLOGY WHITE PAPER

Multi-Service Ethernet Broadband Access Solutions

Combining multi-service and packet-based solutions requires a new way of thinking broadband access and heralds the future of broadband access networks.

Three factors characterize today's broadband access networks. First, the DSLAM and aggregation network are based on ATM switching. Secondly, the service and subscriber intelligence is centralized in the network. And thirdly, the main service offered is high-speed Internet access. This paper will explain how the deployment of new multimedia services (such as broadcast TV, NGN voice services, gaming, etc.) and the concurrent adoption of Ethernet technology require a novel broadband access network design. It explores scalable Ethernet connectivity models for broadband access: the intelligent bridging model and the cross-connect model. For efficient and optimized support of multimedia services, these models should be complemented by multi-media service enablers on the DSLAM, such as service enablers for IP auto-configuration, Quality of Service and multicast. This results in a network architecture where subscriber intelligence and service intelligence are distributed in the access network. These enablers are a first step towards the support of more broadband services that tend to rely as much on communication as on content retrieval.

ALCATEL

Multi-Service Ethernet Broadband Access Solutions

Introduction

DSL technology has become widespread over the past few years and has been adopted worldwide as a means to deliver broadband access. Traditional DSL networks have been built to deliver high-speed Internet access (HSIA) only. Typically, they use ATM switching as aggregation technology. One (or multiple) ATM PVC provides Layer 2 connectivity between the subscriber modem and the Broadband Access Server (BRAS).

However, today, operators are evolving from this initial network architecture. Two factors are driving this evolution. First, fierce competition puts heavy pressure on prices and consequently urges operators towards a CAPEX-optimized network design. Secondly, bandwidth has become a commodity, and the resulting price erosion has advanced the introduction of new services in broadband access. Worldwide, more and more operators are moving towards so-called triple play service offerings including HSIA, video, and voice. These developments also impact the DSL access network. Indeed, taking the service offering beyond HSIA demands increased bandwidths both at the level of the local loop and in the aggregation network. In addition, these new services require new features in the network, such as multicast and quality of service. And therefore, the network also needs to evolve beyond the pure “best-effort” paradigm.

Meanwhile, Ethernet has emerged as an alternative aggregation technology for DSL access. Ethernet is a well established technology in enterprise environments. The main driver for using Ethernet in DSL access has been its promise to deliver high bandwidths at low cost, thanks to the large volumes of Ethernet chipsets. Ethernet for DSL aggregation has already been deployed in Asia-Pacific. But operators in other parts of the world are now taking a closer look at Ethernet aggregation as the technology matures, especially with the latest technology evolutions such as the Virtual Private Wire Service (VPWS) or Virtual Private LAN Service (VPLS) protocols. This paper explains how scalable and carrier-grade multi-service DSL networks can be built using Ethernet aggregation technology.

Section 2 shows the use of Ethernet to deliver high-speed Internet access services. It explains different Layer-2 connectivity options combined with the use of PPP as an auto-configuration technology. Section 3 elaborates on the delivery of new (multimedia) services over an Ethernet aggregation network. While the Layer-2 connectivity options are the same as for high speed Internet access, these new applications put new Quality of Service (QoS) and multicast requirements on the network infrastructure. Furthermore, new services typically no longer rely on the PPP protocol to establish IP connectivity. Instead, they make use of the DHCP protocol. Section 4 discusses how to ensure scalable deployment of Ethernet networks. Section 5 looks forward to further developments, beyond the migration of the Layer-2 aggregation technology towards more services, more bandwidth, and more security. Section 6 provides an overview of the standardization status, and section 7 gives insights into how Alcatel products can deliver solutions outlined in this white paper.

Delivering high-speed Internet access

Delivery of high-speed Internet access to a residential subscriber requires Layer-2 connectivity between the subscriber and the Broadband Remote Access Server (BRAS) (owned either by the network access provider (NAP) or the network service provider (NSP)) and IP connectivity between the subscriber and the NSP (including allocating an IP address to the subscriber). This section introduces two Layer-2 connectivity models for Ethernet access networks: the intelligent bridging model and the cross-connect model. Then it explains how Layer-3 connectivity is established based on the PPP over Ethernet (PPPoE) and PPP protocol.

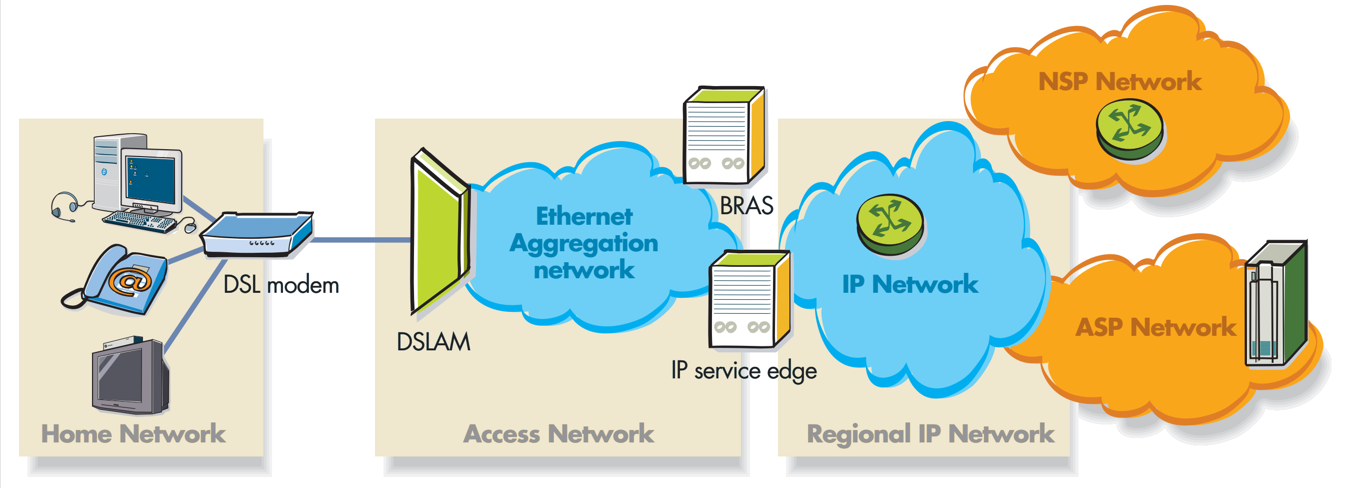
In past ATM-based DSLAMs, all customer-side ATM virtual circuits, connecting the subscriber to the service provider, were cross-connected to upstream virtual circuits. That is, the access multiplexer performed a traffic aggregation function, but the number of logical circuits was left unchanged. This has some advantages, such as preserving customer-specific identifiers and isolating traffic between customers. But it also means that the service provider may end up managing a very large number of virtual circuit instances through the aggregation network.

In Ethernet DSLAMs, a similar cross-connect model will also exist. It is typically employed for connectivity to business customers, especially where the service provider wants to preserve customer VLAN markings across a wide-area network. However a new connectivity model is also available. It is known as Intelligent Bridging. This allows traffic from a large number of individual customers to be consolidated into a single WAN-side VLAN. Typically, there will be a different WAN-side VLAN for the customers associated with each different service edge, and possibly for different service providers, too. But the number of VLAN identifiers used in the aggregation network used for residential traffic is dramatically reduced. The reduced number of VLAN identifiers required simplifies network administration for the operator, because no configuration change occurs within the aggregation network beyond the access multiplexer as individual customers are added or removed from an ‘intelligent bridge’.

Figure 1 shows the DSL network architecture that is assumed throughout this paper.

A DSL modem, located in the customer premises network, is point-to-point connected via DSL to a DSLAM located in the central office. The DSLAM interfaces to an Ethernet aggregation network via one or more Ethernet uplinks. One or multiple edge nodes are located at the edge of the Layer-2 aggregation network. In a typical deployment, the BRAS provides connectivity to the Internet (via the NSP’s network). The BRAS, or a separate IP service edge, provides connectivity to other applications (provided by ASPs).

Fig. 1 **End-to-end network architecture.**



Either ATM or Ethernet can be used as a L2 technology on the DSL line. In the case of ATM, one or more ATM PVCs are configured on the DSL line between the DSL modem and the DSLAM. Different PVCs can be used either for QoS differentiation or service segregation on the last mile. Typically, Ethernet frames will be transported over this ATM connection[1]. In the DSLAM, the ATM PVCs are terminated and the Ethernet frames are extracted. Alternatively, native Ethernet can be transported over the DSL line (without ATM encapsulation), as is the case with Ethernet in the First Mile (EFM) [13]. In the latter case, VLANs can be used for QoS differentiation or service segregation on the last mile.

A standard Ethernet network deploys Ethernet (VLAN) bridging [1], [2]. A VLAN bridge makes use of multiple separate virtual bridge instances. An incoming Ethernet frame is assigned to a particular virtual bridge based on its VLAN-ID. The VLAN-ID is a 12-bit field of the IEEE 802.1Q tag. For untagged frames (i.e., frames that are not 802.1Q tagged), the virtual bridge can be chosen based on either the port on which the Ethernet frame arrived or the Ethertype of the Ethernet frame. Each virtual bridge then performs an independent Ethernet forwarding process, deciding on which bridge (ports) to forward Ethernet frames to, based on the frames' MAC destination address and its own MAC address forwarding table. Traffic cannot be exchanged between two virtual bridges.

To obtain more flexible and more scalable use of VLAN-IDs, the IEEE is currently standardizing stacked VLANs [3]. This allows the tagging of Ethernet frames with two VLAN tags: the original VLAN tag, now called customer VLAN (C-VLAN) tag and a completely new service VLAN (S-VLAN) tag.

DSL aggregation poses some specific challenges for the standard VLAN bridging model. These are best solved at the entry point of the Ethernet aggregation network, i.e., at the DSLAM. The two connectivity models that can be used in a DSL access network - intelligent bridging and cross-connect – are detailed below.

1 It is assumed that Ethernet encapsulations are used on the last mile (PPPoE or IPoE). Other (legacy) encapsulations (PPPoA and IPoA) on the last mile might require additional packet processing in the DSLAM.

Intelligent bridging

Intelligent bridging is based on the Ethernet switching paradigm [1], [2], but introduces a number of enhancements specific for DSL access.

For upstream traffic, the DSLAM assigns the Ethernet frame to a VLAN based on the port/ATM PVC, the VLAN tag (if the frame is already tagged), or the protocol carried inside the Ethernet frame. Next, the virtual bridge corresponding to this VLAN forwards the Ethernet frame to one or more of the Ethernet ports, based on the frame's MAC destination address. The outgoing frame carries a VLAN tag. In the intelligent bridging model, traffic from multiple subscribers gets VLAN tagged with the same VLAN-ID. Typically, the VLAN-ID will be unique per DSLAM or per DSLAM-edge node pair (not per subscriber).

The VLAN tag that is applied is either a customer VLAN tag (C-TAG) [2], or a service VLAN tag (S-TAG) [3]. Both tags have an identical structure, but are identified by a different Ethertype. C-VLANs will be used in combination with legacy VLAN-aware Ethernet switches in the aggregation network, while S-VLANs will be deployed in future "provider-bridged" networks. It is also possible to apply a so-called VLAN stack [3] i.e., a combination of a C-VLAN and an S-VLAN. This last solution makes it possible, for example, to use the C-VLAN tag for service differentiation on the last mile. Figure 2 shows an example of the intelligent bridging model. The protocol stack on the left side illustrates the ATM encapsulation on the last mile and the transmission of Ethernet frames on the uplink. The right side shows that Ethernet traffic from the black and the red PVC gets tagged with a blue VLAN (VLAN 1), while traffic from the blue PVC gets tagged with an orange VLAN (VLAN 2).

Fig. 2 **Intelligent bridging model.**

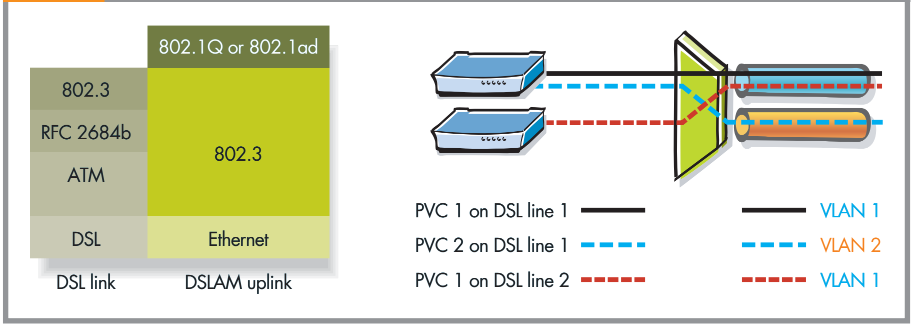
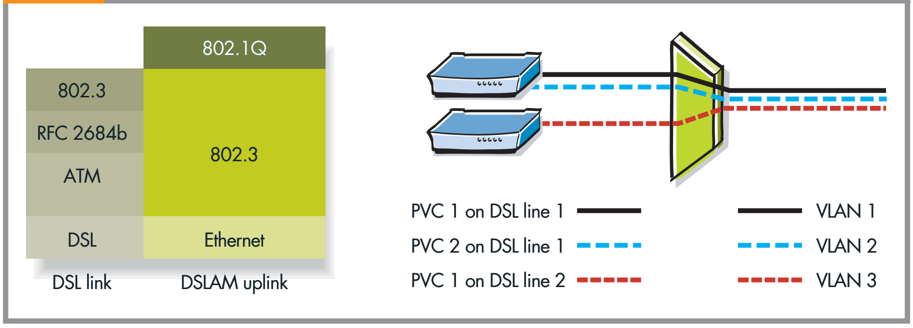


Fig. 3 **Cross-connect model.**



In addition, the DSLAM will implement a number of security enhancements. To protect end-users against service degradation or denial of service resulting from MAC address spoofing, the subscribers are not allowed to have direct L2 connectivity at the DSLAM level, i.e., L2 connectivity between users is blocked in the DSLAM. Subscriber communication is only allowed at Layer 3. Hence, all upstream traffic is sent first to the edge (the BRAS for HSIA traffic) where the traffic can be policed and accounted for. This is achieved by having a PPPoE session established between the subscribers and the BRAS at IP connection set-up.

Secondly, the DSLAM needs intelligent filters on broadcast/multicast traffic to prevent broadcast storms and malicious use of Ethernet control messages. Indeed, in the upstream direction, the DSLAM is located at the ingress of the network and should discard subscriber multicast and broadcast traffic to protect the DSLAM itself as well as the Ethernet aggregation network. However, a number of control protocols (PPPoE, DCHP, IGMP, ARP, etc.) make use of broadcast/multicast messages. Hence, the DSLAM will need some intelligence to filter out those messages and process them appropriately. Similarly, downstream broadcast messages should never be sent on all DSL lines and should be discarded (except for some control layer protocols).

Additional security filters in the DSLAM limit the number of MAC addresses in use on a particular DSL line and prevent MAC address spoofing (the use of the same MAC address on a different DSL line).

Cross-connect model

In the cross-connect model, the DSLAM maps all traffic from a particular ATM PVC (or DSL port) onto a unique VLAN-ID (unique within the realm of the L2 aggregation network). In other words, there is a one-to-one mapping between an ATM PVC (or DSL port) and a VLAN-ID. The cross-connect model in fact mimics the connection-oriented nature of ATM over an Ethernet aggregation network. Because of the one-to-one mapping, forwarding of Ethernet frames in the DSLAM becomes straightforward, and MAC address learning in the DSLAM is not strictly required[2]. Figure 3 shows an example of the cross-connect model. Traffic from PVC 1 on the first DSL line is cross-connected to VLAN1. Traffic from PVC 2 on the same DSL line is cross-connected to VLAN2. Finally, traffic from PVC 1 on a second DSL line is cross-connected to VLAN3.

2 Except for multipoint Ethernet LAN services (E-LAN services as defined by the Metro Ethernet Forum).

Due to the limited number of VLAN IDs, 4094 (12 bits within the 1Q tag, two values reserved), this model has inherent scalability problems when it is used to offer connectivity to residential subscribers. Usually, the number of subscriber within an L2 aggregation network is larger than 4094. This scalability problem can be solved by enhancing the Ethernet aggregation network with MPLS switching, offering VPWS and VPLS tunnels. This simplifies the network architecture by keeping the VLAN IDs only locally significant on the Ethernet uplink between the DSLAM and the first aggregation network switch.

A second solution for this scalability problem is to apply VLAN stacking, i.e., a customer Ethernet frame is then mapped to a unique VLAN stack. This gives a unique combination of a C-VLAN-ID and an S-VLAN-ID [3].

Typically the S-VLAN will be unique per DSLAM or per DSLAM-edge pair, and for a given S-VLAN or DSLAM all C-VLANs are unique. The use of a VLAN stack therefore allows 4094 DSLAMs and, for each DSLAM, 4094 subscribers. If the number of subscribers on a DSLAM exceeds 4094, an extra S-VLAN can be allocated.

The cross-connect model is often used for offering Ethernet LAN (E-LAN) and Ethernet LINE (E-LINE) services to small and medium-sized enterprises (SMEs) and small office/home office (SOHO) enterprises. These services have been defined by the Metro Ethernet Forum (MEF). Both services mediate the exchange of Ethernet frames between customer devices or between customer devices and a service edge. The E-Line services are point-to-point services, and the E-LAN services are multipoint-to-multipoint services. E-Line services can be used for providing HSIA, connection with voice gateways and edge routers for IP-VPN services, as well as site-to-site connectivity. E-LAN services are mostly used for multi-site connectivity. When these services are offered, it is possible that the frames from the CPE are already tagged. If VLAN-ID transparency is required, i.e., the service leaves the customer VLAN unaltered, then the DSLAM will leave the VLAN-ID unmodified and may stack an S-VLAN.

Therefore, the number of S-VLANs available to segregate DSLAMs is, in practice, smaller than 4094 due to the fact that S-VLANs are also used to segregate business services. Each Ethernet LAN and Ethernet LINE business service requires one S-VLAN. Hence, for large aggregation networks, 4094 S-VLANs might still not be sufficient. This scalability issue arises both in the intelligent bridging and in the cross-connect model. Section 4 explains how scalable deployment can still be achieved.

Finally, it should be noted that the intelligent bridging and cross-connect models are often deployed simultaneously, even within the same DSLAM. The intelligent bridging model is then, for example, used for residential services, where traffic from multiple subscribers is aggregated into one VLAN. Traffic from SME/SOHO subscribers is cross-connected and isolated on Layer 2 from the residential traffic.

Delivering high-speed Internet services over PPPoE and PPPoA

IP connectivity between the home terminal and the Internet Service Provider (ISP) for HSIA will typically be established by using the PPPoE protocol [4]. The auto-configuration proceeds in two phases. In a first phase, PPPoE allows a point-to-point session to be set up between the modem or terminal and the BRAS. In a second phase, the PPP protocol [5] is used to establish IP connectivity, authentication, and service selection.

For security, accounting, and troubleshooting reasons, it is often desirable to link the BRAS and/or AAA infrastructure to a PPP session with a particular DSL line. This allows RADIUS logs to be perused based on an IP address or a user name to find out which DSL line was used under the particular circumstances under examination.

For a cross-connect model, this is straightforward, since there is a one-to-one correspondence between an ATM PVC on a particular DSL line and a C-VLAN-ID or C-VLAN-ID/S-VLAN-ID combination. Therefore, the DSL line information is preserved in the aggregation network. In an intelligent bridging model, this information is lost, since traffic from multiple PVCs is aggregated into the same VLAN-ID. However, it is possible to dynamically link the PPP session to a particular DSL line or PVC by introducing a so-called PPPoE intermediate agent in the DSLAM [9]. This intermediate agent will add a line identification field to some of the session initialization messages exchanged between the PPPoE client and server during the PPPoE session setup. By interpreting this field, the PPPoE server (i.e., the BRAS) can determine which DSL line is setting up a new PPPoE session.

Although PPPoE is the preferred connectivity mechanism for HSIA, some legacy modems might still use PPPoA auto-configuration. Backwards compatibility requires that these modems also be supported in an Ethernet aggregation network. The most straightforward solution is to implement a PPPoA-to-PPPoE translation in the DSLAM.

The use of PPP as an auto-configuration technology shortcuts the connectionless nature of the Ethernet network that runs underneath. Indeed, all IP traffic carried over the PPPoE session will always flow directly from the home terminal towards the BRAS, thereby avoiding a number of security threats mentioned earlier. The threat of MAC address spoofing is minimized because subscribers cannot have a direct communication at the Ethernet layer. The IP traffic will always be transported to the BRAS over the PPP connection. This guarantees that traffic from peer-to-peer applications over the Internet will always pass through the BRAS (where proper accounting can be done).

Finally, it should be noted that DHCP can also be used as an alternative to PPP for HSIA, allowing a much easier IP configuration of the terminals and thereby reducing support needs for end-users. This alternative is particularly attractive for Competitive Local Exchange Carriers (CLEC) or providers that do not have wholesale requirements. Indeed, PPP for wholesale Internet access is a well established and embedded delivery model which service providers see no compelling reason to change for now.

Delivering multimedia services

For the past couple of years, network and service providers have been looking to increase their revenues from broadband access networks by offering multimedia services to their broadband subscribers. The multimedia service offering ranges from broadcast TV and video, Video on Demand (VOD), to NGN voice services and online gaming. These new multimedia services have a number of characteristics that set them apart from high-speed Internet access.

Characteristics of multimedia services

The first important characteristic of multimedia services is that, in most cases, they are delivered from terminals other than PCs. Examples of multimedia terminals are set-top boxes, SIP phones, television sets, and gaming consoles.

The second characteristic of multimedia services is that, although they are IP-based services like HSIA, they obtain their IP configuration parameters by protocols other than PPP. These protocols are, for example, Dynamic Host Configuration Protocol (DHCP), Internet Group Management Protocol (IGMP) and Address Resolution Protocol (ARP).

The third characteristic of multimedia services is that, contrary to HSIA, most of them are interactive session-based services[3]. These sessions can be established between two or many peers, the peer being a server or another broadband subscriber.

[3] Session-based at the application level like a telephone call, a gaming session, a video download,…

Finally, multimedia services require quality and availability guarantees for the service delivery. These requirements can be either regulatory (such as for emergency calls), imposed by the technical specifications of the service (such as delay and jitter), or influenced by the competitive ways of accessing the same service. Indeed, broadcast TV on broadband DSL is in direct competition with cable and satellite television, while VOD service must be able to compete with DVD rentals or NGN with analog voice or mobile services.

Moreover, the adoption of Ethernet in the access network also allows network providers to offer Ethernet Virtual Private LAN services over DSL to small and medium enterprises, the so-called E-line and E-LAN services defined by the MEF. These services are usually based on service level agreements, including requirements on quality of service, reliability, and availability that go beyond the service guarantees offered to residential subscribers.

So support of the above multimedia services requires new auto-configuration architectures that are not based on PPP and that can manage multiple terminals in the home. It also requires new connectivity models such as multicast and a quality of service scheme in the access network.

As a consequence, an Ethernet broadband access solution that is optimized for multimedia service support will implement a number of multimedia service enablers in the access network that facilitate and optimize the deployment of these services. The most important multimedia service enablers for the Ethernet broadband access multiplexers will be described in the following paragraphs.

Service enablers for IP auto-configuration in Ethernet broadband access

Multi-media terminals such as set-top boxes or IP phones request an IP address from the service provider by means of the DHCP protocol. The use of DHCP in a DSL context makes sense since the protocol allows connectivity establishment to be separated from data path forwarding (as opposed to PPP). This results in a simple and scalable solution. Furthermore, DHCP-based auto-configuration allows for easy support of QoS and multicast in the access network. In a PPP model, the PPP protocol demands that the stream of IP packets leaving the PPP connection be the same as the stream of IP packets entering the PPP connection. Hence, PPP prohibits reordering of packets or the insertion of new packets in the PPP connection somewhere between the PPP client and server. This hampers deployment of QoS and multicast in the access network. The DHCP-based auto-configuration protocol is better suited to support network-based QoS and multicast, since DHCP does not have the same restrictions as PPP. However, when DHCP is used in a DSL context, appropriate interworking with the AAA system needs to be foreseen [6].

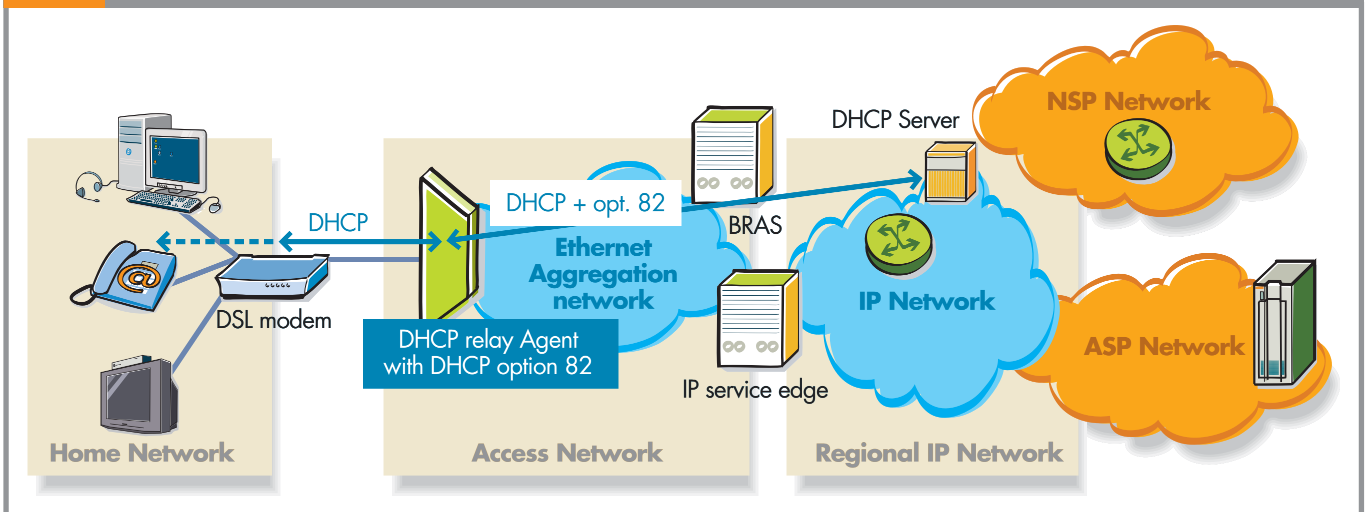
With the deployment of DHCP in an Ethernet access network, the connectionless nature of the Ethernet aggregation network has to be taken into account. Indeed, in the intelligent bridging model, the relationship between a subscriber (identified by the subscriber line) and its Ethernet frames is lost upstream of the DSLAM in the Ethernet aggregation network. This relationship may be used for a number of authentication, security, troubleshooting, and accounting functions (as described above for PPPoE).

It is therefore preferable to implement a number of auto-configuration related functions on the DSLAM.

The service enablers for IP auto-configuration to be implemented on the Ethernet DSLAM are the following:

1) A DHCP relay agent inserting the DSL line identifier (option 82) as described in [7] and shown in Figure 4. The advantage of having the DHCP relay on the DSLAM rather than on the IP edge node is that it takes away the

Fig. 4 **DHCP session establishment (with access node implementing full DHCP Relay Agent)**



issues of upstream and downstream DHCP broadcast messages on the network. Such DSL line identification proves to be very useful for several reasons:

- Authentication: RADIUS authentication & accounting is sometimes performed based on such DSL line identification. In a retail environment, this could be used to identify the subscriber and to figure out which service parameters should be returned to the BRAS (via the RADIUS authorization process). In a wholesale environment, this could be used to check the domain name in the user credentials and verify that it is compatible with the ISP (or list of ISPs) that required the establishment of a service (e.g., Internet access or more) on this DSL line.
- Troubleshooting: the line information can be used for troubleshooting. It allows the perusal of RADIUS logs based on an IP address or a user name to find out which DSL line was used under particular circumstances under examination.

2) An IEEE_802.1X authenticator provides strong and secure port-based authentication. This authenticator should be implemented on the DSLAM if the authentication provided by the DHCP option 82 (line ID) is considered insufficient, see also Figure 5. The IEEE 802.1X standard [8] specifies a mechanism to transport Extensible Authentication Protocol (EAP) messages between an Ethernet-capable terminal (Supplicant) and an Ethernet switch (Authenticator) to which it is connected, using RADIUS for example. The Authenticator controls the operational state of its controlled ports based on the outcome of the authentication process.

To correlate the 802.1X authentication by the access provider and the DHCP IP address allocation by the NSP, new proposals have been made at the IETF [11] that would allow the insertion of a RADIUS attribute (e.g., the authentication result) in option 82 next to the line ID in the DHCP DISCOVER messages. This ensures that the DHCP server knows the result of the 802.1X authentication.

Note also that the multiplication of terminals in the home and the different requirements from the various broadband applications make management of the home network and gateway something of a nightmare for most broadband subscribers. It has therefore become clear that the configuration of the home network by the network and service providers should go beyond the IP-layer service auto-configuration. Different standardization efforts and product developments are in process here with the objective of guaranteeing a plug & play environment for the end-user [12].

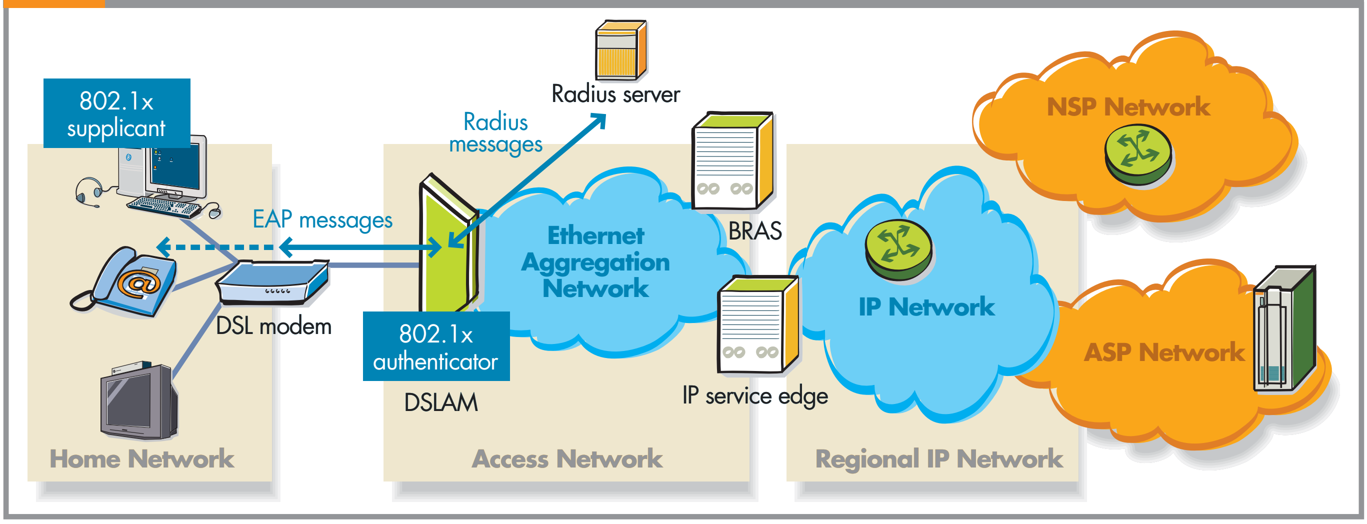
Service enablers for IP and Ethernet multicasting

The delivery of broadcast TV or video services over DSL relies on IP multicast mechanisms. Instead of broadcasting the content streams to everyone in the network (as happens in cable and satellite), the end-user joins a multicast group by selecting a channel. Duplication of the channel towards this end user will last as long as the end-user is interested in receiving the channel.

From a technical point of view, this is achieved by using the IGMP protocol. A user who wants to watch a channel, will send an IGMP join message for the multicast group identifying this channel. He will continue to send IGMP control messages for the whole duration of the session with the content server.

To optimize the multicast service delivery, attempts need to be made to minimize first the network reaction time for a channel change, second the bandwidth usage for duplicated streams, and finally the exchange of control messages between the user, the network elements, and the content server. Figure 6 illustrates a multicast

Fig. 5 802.1X authentication message sequence

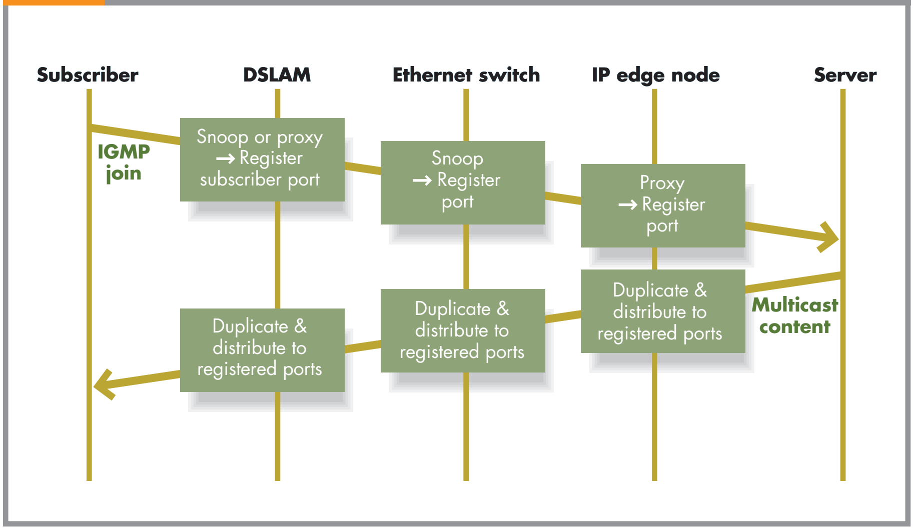


architecture for an Ethernet broadband network that complies with these requirements and makes full use of the multicast duplication capabilities of an Ethernet network.

There is essentially only one mode of operation for multicast in a bridging DSLAM: participants are added to or removed from multicast group lists based on the detection of IGMP messages in the upstream traffic. The only nuance is that these IGMP messages can either be passed on into the network with their original source address (snooping), or the IGMP messages can be proxied by the DSLAM. If proxied, only the IGMP messages which are relevant to the next node will be passed on - a request from a customer for a channel which is already being sent to that access multiplexer would be discarded, since the channel is already available. In both cases, the upstream IGMP messages will always be VLAN-tagged, as required to segregate traffic on the aggregation network. Within the aggregation network, the IGMP messages are snooped by bridges to optimize the Layer-2 multicast distribution tree.

In the DSLAM, downstream multicast traffic will be duplicated to all interested ports (subscriber port or a subtending DSLAM port).

Fig. 6 **Multicast architecture for the intelligent bridging model.**



The multicast service enabler on the DSLAM will thus implement the following functions:

- for every (remote) user port, keep track of multicast group membership status and duplicate traffic as appropriate,
- filter out redundant IGMP messages,
- select the appropriate VLAN for upstream IGMP traffic,
- for a DSLAM with IGMP proxying, keep track of available multicast groups, request or leave multicast groups as appropriate.

A related question is if authorization and accounting for broadcast services is required in the DSLAM. In current implementations, encryption of content streams by the server guarantees that only the registered users can decrypt the stream as they know the key. A malicious user could join a channel on which he is not authorized, but he will not be able to decrypt it.

However, it is possible that future implementations will also require authorization and accounting for broadcast services in the DSLAM. Appropriate authorization and accounting enablers need then to be implemented.

Service enablers for Quality-of-Service and resilience in the Ethernet broadband access

Quality-of-Service schemes for Ethernet networks are still in their infancy. There is no in-band signaling defined for resource reservation in Ethernet, nor is there a mechanism for off-line traffic engineering. So implementing QoS guarantees in an Ethernet network requires a resource controller that can reserve resources and do call admission control.

One way of reserving resources in an Ethernet network is to associate a certain bandwidth and scheduling priority to a VLAN ID and IEEE 802.1p priority bit pair in each of the switches of the network. This allows the creation of a simplified overlay network view in terms of QoS pipes that can then be used by the resource controller for classifying and admitting a call.

For this model with QoS pipes to work, predictable behavior should be enforced in the network by implementing functions that ensure congestion avoidance for traffic with QoS guarantees. Three types of functions are needed to accomplish this: per hop scheduling and queuing functions, traffic classification functions, and traffic policing functions. These functions are needed in the home gateway in the customer network, as well as in the access node, Ethernet switches, and IP edges as is explained below.

To fulfill the delay and packet loss requirements of certain classes of traffic, appropriate **traffic queuing and scheduling functions** are needed in all the network elements. The queuing and scheduling is done hop by hop, both in upstream and downstream, and is based on the traffic class or QoS class of the packet. In IP network elements, the traffic class can be identified by its Type-of-Service (ToS) bits, by the traffic type (TCP or UDP), or by a combination of source and destination IP address. In Ethernet network elements, the traffic class is identified by the priority bits (p-bits) or VLAN ID of the frames. Different scheduling methods can be applied, e.g. strict priority and weighted-round-robin. When p-bits are combined with VLAN ID for indicating QoS classes, the network elements should have the ability to queue in function of the VLAN ID.

Furthermore, in case of congestion, a mechanism for selectively discarding frames should be in place. Weighted Random Early Discard (WRED) on the queues allows packets to be dropped based on drop precedence such that higher priority packets are less likely to be dropped during network congestion.

However, the WRED mechanism cannot be applied today in standard Ethernet switches as there is no drop precedence indication in the p-bits. This issue is under consideration in standardization.

Implementing queuing and scheduling in function of the traffic classes requires that the traffic first be classified and marked. Therefore **Traffic classification functions** are required at ingress points of the access provider network. These functions ensure, first, that traffic requiring a preferred treatment is classified in the correct QoS class, i.e., assigning priority to different flows of traffic depending on how critical and delay-sensitive they are, and second, that packets are marked accordingly at all layers of the protocol stack. This requires a subtle inter-working between application, IP, Ethernet, or ATM QoS prescriptions.

For upstream traffic, classification functions must be present on the access node and in the home gateway.

The most interesting classification model is based on a classification of traffic in the home gateway in function of the requirements of the applications the user has subscribed to, and a further classification in the access node to comply with the SLA and to ensure interworking between different technologies present in the access network (from ATM to Ethernet, from IP to Ethernet).

For downstream traffic, classification and marking of the traffic will be done at the service edge (e.g., BRAS) or on ingress to the aggregation network.

There are two ways of using VLAN tags for marking the traffic class of Ethernet frames. The first is to use the VLAN ID only for connectivity and DSLAM segregation as shown in the intelligent bridging and cross-connect models above (see sections 2.1. and 2.2). In that case, the IEEE 802.1p priority bits need to indicate the Class of Service (CoS). This is the equivalent to the use of an E-LSP in MPLS.

The second way is to use a separate VLAN tag per service or per CoS class. It offers more fine-grained control over the transported traffic because, in Ethernet, different VLANs can be mapped to different spanning trees. However this solution consumes more VLAN IDs.

Concerning the management of the QoS functions on the home gateway, a promising model is described in the new DSLF Technical Report TR69 and Working Text WT98 from the DSL HOME Working Group. This model is based on remote management of the home gateway by a provider-owned Auto-Configuration Server (ACS) that, among other things, configures the QoS classification and traffic marking to be associated with each application that the user has subscribed to, as well as the scheduling parameters.

Note also that the configuration of the home GW by the ACS can be renewed each time the user subscribes to a new application.

Traffic policing functions ensure that users of a network comply with the traffic profile agreed with the network operator in the service level agreement. These functions include traffic shaping.

If the above ACS model is applied, the marking of upstream traffic can be trusted by the access node, because the management is done by the provider.

However, policing of upstream must still be done in the access node. First, upstream policing of individual traffic is still required by the access provider if the ACS does not belong to the NAP or if the NAP has no assurance that the user cannot tamper with the settings. Second, to ensure strict QoS guarantees, the DSLAM needs to perform bandwidth control at the ingress of the Ethernet network. Bandwidth control can be done by per VLAN (or S-VLAN) or per class policing and shaping at the ingress of the Ethernet network. Stricter guarantees can be provided with policing at the ingress port of each Ethernet switch. The service edge and the access node must also implement policers and shapers for downstream traffic.

Once all the above QoS enforcement functions are in place, the network operator should dimension the network and the QoS pipes, set the QoS parameters in the network elements, and implement call-admission control for each new application session requiring Quality of Service. A promising mechanism is the one currently defined in ETSI-TISPAN standardization , which is translating the 3GPP IMS model for a fixed access network. This model relies on a resource controller that is triggered by application signaling and can thereby offer the QoS required by a given application and for the duration of a session. The resource controller is further responsible for reserving and controlling the network resources.

Service guarantees also require service availability and therefore a **mechanism for network resilience**.

In the Ethernet aggregation network, resilience is achieved by spanning-tree reconfiguration. Whenever a link, port, or switch fails, the spanning tree will automatically reconfigure to regain loop-free connectivity. All network elements, including the DSLAM, will implement the standard Rapid Spanning Tree Protocol (RSTP). Depending on the size of the network, the configurations of weights on switches and ports, and the type of failure, restoration times between 50ms and 5s can be achieved.

Moreover, on the DSLAM itself, the protection mechanism known as link aggregation (IEEE_802.3ad) may also be implemented. Link aggregation allows for the distribution of traffic over different parallel physical links as if they were one

Ethernet link and thereby offers a seamless protection scheme if one of the links fails. It should be noted that link aggregation does not protect the DSLAM traffic against failure of the Ethernet switch it is attached to. It is therefore not recommended as a unique protection solution when offering multimedia services.

On top of the Ethernet resilience functions implemented in the DSLAM, the Ethernet aggregation network, when implementing MPLS transport, can make use of MPLS Fast Reroute restoration techniques.

It is important to highlight that better results for QoS and resilience, both in terms of performance and monitoring, can be achieved if the Ethernet aggregation network relies on Ethernet over MPLS solutions such as Virtual Private Wire Service (VPWS) or Virtual Private LAN Service (VPLS).

Scalable network deployments and end-to-end solutions

The previous sections described the intelligent bridging and cross-connect models as well as the service enablers to be implemented in the DSLAM for the deployment of multimedia services.

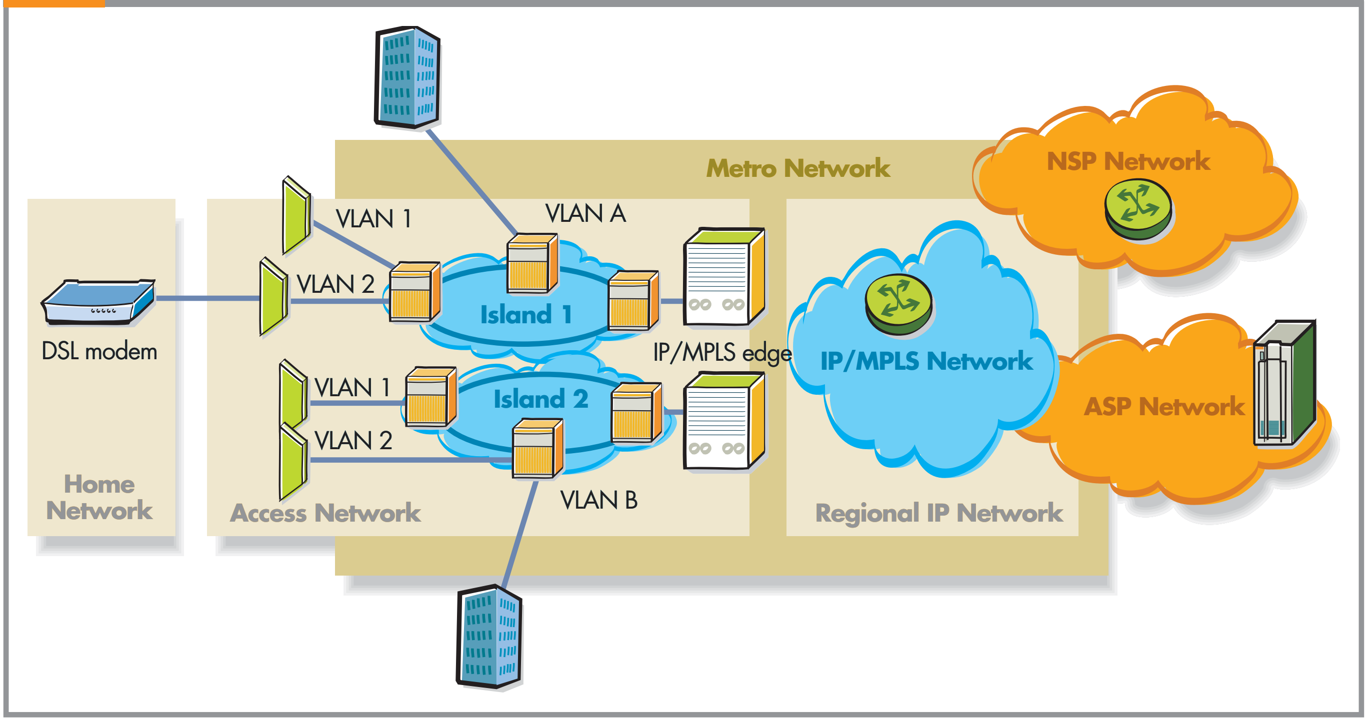
This section explains how to deploy a scalable network solution based on the above elements. Ethernet switching presents a number of limitations in terms of scalability, most notably in terms of VLAN tags and MAC addresses. The VLAN tag is limited to 12 bits, giving a maximum of 4094 different tag values[4]. As has been explained, in Ethernet access networks, the VLAN tags are used to identify DSLAM-edge pairs as well as individual Ethernet business services. Some access networks are very large and serve a very large number of (business and residential) customers. Consequently, 4094 VLAN ID's may not be sufficient. Moreover, a large number of subscribers implies that the MAC address tables of the Ethernet switches in the aggregation network can become very large.

As explained earlier in section 2, VLAN stacking does not solve the S-VLAN scalability problem, because in practice the number of S-VLANs available to segregate DSLAMs is limited by the fact that S-VLANs are also used for Ethernet LAN and Ethernet LINE services to business customers. Each Ethernet LAN/LINE service consumes one S-VLAN.

For delivery of broadband services to residential customers, a scalable solution can be obtained by keeping the Ethernet aggregation network small. A number of so-called Ethernet islands, i.e., separate Ethernet aggregation networks, are created, separated by an IP router or a BRAS as illustrated in Figure 7. Within each island, the whole range of VLAN IDs can be used. In addition, MAC addresses from subscribers attached to one island are not visible in other aggregation networks, such that MAC address tables and ARP tables in Ethernet switches and in the IP edge can be kept at reasonable sizes. Another advantage of this solution is that it provides an easy way to limit the broadcast domains inside the Ethernet network. The size of an island is determined by the scalability of the Ethernet switches that are deployed, the scalability of the edge/BRAS in terms of number of sessions, and the number of aggregation networks per IP edge.

[4] Two values are reserved.

Fig. 7 Scalable Ethernet access networks via VLAN islands



Scalability can be further improved by introducing IP forwarding functionality at the level of the access multiplexer, such that a single access multiplexer becomes an Ethernet island. In such a model, subscriber MAC addresses are not propagated on the Ethernet aggregation network, but instead subscriber Ethernet frames are terminated in a IP forwarder in the access multiplexer. The latter approach also improves the robustness of the network against Layer-2 security attacks, since subscriber Ethernet broadcast/multicast frames are not propagated within the aggregation network. However, a full discussion of this model is beyond the scope of this paper.

For delivery of Ethernet LAN business services (E-LAN and E-line services), the Ethernet islands do not provide any relief. Indeed, the nature of the service is to transport the customer's Ethernet frames unaltered between two business customers. The customer sites connected by an Ethernet service do not always reside in the same Ethernet island. Moreover, the operator cannot route the customer Ethernet frames at the edge of the network.

The best solution is to encapsulate the Ethernet frames in MPLS at the IP edge (via a VPWS or VPLS solution). This requires an IP edge (BRAS or IP service router) that supports VPWS or VPLS. Ethernet frames are then transported over MPLS tunnels between the different Ethernet aggregation networks. Within each island, the provider can use the full range of VLAN (S-VLAN) tags, as these are not transported over the MPLS tunnel.

The size of the MPLS network and the respective Ethernet islands may vary in function of the scalability and service quality requirements of the network operator. A highly scalable and efficient solution is to have MPLS switching already in the aggregation network, which has the additional advantage of offering QoS, high availability, and good service segregation in the whole access and metro network.

Finally, as an illustration, the following typical deployment scenario can be considered. The number of residential subscribers per DSLAM varies from a few hundred to a couple of thousand. SME/SOHO customers will typically also access the network via DSLAMs or other residential access nodes for permanent Internet access and Ethernet LAN interconnections. Large enterprises will access the network via dedicated fiber access on a provider edge switch. The number of residential subscribers per BRAS ranges from 10,000 to 100,000. With 1 to 10 Ethernet islands per BRAS, this means that the number of VLANs per island for residential services will be in the order of 100 VLANs. This leaves enough VLANs for the business Ethernet services.

In the above configuration, the number of residential subscribers per Ethernet island will be around 10,000. Typically, the residential customer will use one or a few MAC addresses, and up to 10 for SME/SOHO subscribers. Large enterprises and many SMEs use a routed modem, so terminal MAC addresses will not be visible in the network.

Future developments

Future developments of multi-service packet-based broadband solutions are expected to happen in four directions: more services, more intelligence, more bandwidth, and more security.

More services

It is clear that multimedia services are not restricted to video, voice, and gaming services. Regularly, new broadband applications appear, with a very clear tendency to rely as much on communication as on content retrieval. Examples of these new services are interactive TV, peer-to-peer applications, and personal video broadcasting. The communication and interactivity aspect is what makes online multimedia services so special with respect to traditional media such as broadcast television or DVD. Therefore, easy and efficient ways of establishing reliable and interactive broadband communications between one or multiple peers will become extremely important.

More intelligence

Access solutions should be optimized for these new services. As all multimedia services are IP-based, this optimization can be achieved by increasing the IP intelligence of the access network, which means adding even more multi-media service enablers on the access platforms. Furthermore, an increasing demand for multimedia services will also require more scalability in terms of management, operations, and equipment. Such scalability improvements will be obtained by introducing IP forwarding in the access node.

As a result, DSLAMs or access platforms optimized for multimedia services will have more and more service and subscriber intelligence. And they will rely mostly on IP functions for handling the multi-media traffic, while keeping the more straightforward Intelligent Ethernet switching for providing either HSIA, Layer-2 or Layer-3 wholesaling to third party NSP.

This evolution parallels that of the Network Access Provider taking up a new role as Network Service Provider and offering application wholesale to its customers with optimized service delivery in terms of QoS, multicast, etc.

More bandwidth

The uptake of multi-media services fuels the end-user demand for more (symmetrical) bandwidth. Indeed, the interactive broadband applications mentioned above have symmetrical traffic patterns in upstream and downstream. New, higher bandwidth DSL PHYs (ADSL2+, VDSL, 10PASS-TS, VDSL2, etc.) can provide this bandwidth. PHYs of the VDSL family can also offer more symmetric bandwidth.

As higher bandwidths imply shorter copper loops, the introduction of these new DSL PHYs will be accompanied by the roll-out of fiber deeper in the network and the introduction of remote units located much closer to the users. The intelligent bridging and cross-connect connectivity models can also be applied to these remote unit network architectures. Furthermore, the deployment of remote unit architectures will accelerate the need for scalable fiber aggregation platforms in the central office. These platforms will implement many of the service enablers described earlier, as their implementation on remote units may not be cost-efficient.

More network security

As explained above, security features are needed on the DSLAM to protect both the DSLAM itself and the provider's network, and the other subscribers from attacks. It is expected that in the future, the security features to protect the provider's network and other subscribers from higher layer attacks will be enhanced. Indeed, the DSLAM or the access provider edge node will be required to perform more and more security checks as soon as new traffic enters the network, given that many attacks, such as Denial of Service (DoS) and Distributed Denial of Service (DDoS), can be prevented that way. This evolution is driven by two factors. First, the DSLAM is becoming more and more IP aware and in an IP network, security checks should be done at the ingress of the network because of the connectionless nature of the technology. The second factor is that new security regulations recognize certain responsibility of the providers in the security of the network and the end-user. Examples of security enhancements are generic MAC/IP filters, associated with policy management.

Standardization perspective

Standardization of new solutions is very important. It is an essential step towards interoperability of equipment and solutions from different vendors. As a result, it also lowers the barriers for adoption of new solutions both by network operators and by end-users and accelerates the adoption of new broadband services. Alcatel is therefore investing a lot of effort in standardization related to multi-service broadband access solutions.

Alcatel is active in the DSL Forum Architecture & Transport working group and DSL Home working group. Here, very interesting developments are in process concerning architectures for Ethernet broadband networks with a migration perspective from ATM as well as remote management of the home network for plug & play multi-service deployments.

Alcatel is also contributing to developments in ITU-T SG15/Q12, SG16/QB, and SG13/NGN Focus Group. These are working on standardization of detailed functional architectures for broadband solutions and services as well as the related management, starting from the high-level architectural views (for example, from the DSLF) and aiming at real interoperability.

Besides the functional and architectural specifications, Alcatel is also leading and contributing to the development of new protocols and elements that make up the multimedia packet-based solutions in IEEE_802.1 and IEEE_802.3 as well as in the Metro Ethernet Forum (MEF) and the IETF.

Alcatel is also very active in the new ETSI group called TISPAN, whose goal is to adapt the IP-Multimedia Sub-system (IMS) - defined for mobile networks by 3GPP - to fixed broadband access networks.

Additionally, the Alcatel Research and Innovation team focusing on broadband access is also leading a European research consortium, named MUSE [14], whose aim is to push the multi-service properties of the packet-based solutions even further and to accelerate the development of standardized solutions.

Alcatel products at a glance

The evolution towards multi-service packet-based aggregation networks has an important impact on the role of the DSLAM. Indeed, the new architectures not only introduce new types of interface on the DSLAM, they also demand a rethink of the position of several key functions in an access network and hence the functionality of a DSLAM.

To meet the requirements of this new network environment, the Alcatel DSLAM product portfolio and the feature set of each specific product is continuously evolving. A first step was taken over two years ago with the introduction of the Fast Ethernet uplink on the Alcatel 7300 ASAM. Since then, this product has been further extended to support multiple forwarding models and to take up its role in subscriber management and security solutions. The Alcatel 7300 ASAM with Fast Ethernet uplink is today widely deployed (several million lines), in particular as a solution for offering high-speed Internet access via Ethernet aggregation.

A next generation of DSLAM was introduced with the 7301 ASAM, optimized for a multi-media environment and providing a range of dedicated features to enable efficient deployment of video services. In addition, the 7301 ASAM is positioned to fit in the environment of gradual network transition from ATM to Ethernet/IP, as it supports a mix of uplinks (Ethernet + ATM) in a single system. The GigE interface is initially designed with focus on the infeed of video channels. In the near future the GigE on 7301 ASAM will evolve further from a Layer-2 (Ethernet) solution to an L3 (IP) solution, including dedicated protocol support for the different access scenarios that are encountered in a typical multi-service multi-edge environment, as well as the associated QoS and security support.

The 7302 ISAM marks a new step in the evolution of the DSLAMs towards the new network architectures and provides a future-safe platform for a true full-service environment. Equipped with intelligent line cards and with a non-blocking internal capacity of 24 Gbits/s per shelf, this platform will become the cornerstone in the new full-service networks. As for the other products, the further evolution of the 7302 ISAM in different domains (IP & Ethernet, but also new DSL technologies, etc.) will ensure that the challenges of an ever changing IP environment will be met.

This product portfolio is further complemented with a set of smaller nodes which can be deployed as remote nodes, for example, in a subtending configuration. Each of these also plays its own role in IP and thereby opens the way to a network architecture with maximum flexibility in terms of distributing IP intelligence.

Last but not least, other than their IP support, the Alcatel DSLAM remains the best in class in many other functional domains, such as the support for a variety of DSL flavors and advanced management solutions.

In addition to new access products, Alcatel also provides Ethernet aggregation and service edge devices, the 7450 ESS and 7750 SR, as part of its multi-service Ethernet broadband access solutions. The 7450 ESS and 7750 SR combine Ethernet and MPLS technologies to deliver a highly available, traffic-engineered aggregation network. Hierarchical QoS and service-aware OAM tools enable accurate per-service bandwidth enforcement and extensive troubleshooting capabilities. The combination of Ethernet and MPLS with service-oriented products also allows service providers to leverage a common Ethernet aggregation network for both residential and business services.

Conclusion

The migration to Ethernet, and more generally packet-based technologies, in broadband access is motivated not only by cost and technology arguments, but mainly by the desire of network operators to offer their subscribers multimedia services next to high-speed Internet access. New multimedia services rely as much on communication as on content retrieval. The communication and interactivity aspect is what makes online multimedia services so special compared to traditional media.

The paper has first described Ethernet connectivity models that are needed for delivering the basic high-speed Internet service: the intelligent bridging model and the cross-connect model. Both models rely on standard IEEE802.1Q bridging but require additional security enhancements. These models will probably be used in parallel in order to serve different purposes. The intelligent bridging model is more appropriate for offering services to the residential subscribers, whereas the cross-connect model is more appropriate for offering Ethernet LAN and Ethernet LINE services to small and medium-sized enterprises.

Special attention was paid to the deployment of scalable Ethernet solutions, taking into account the scale limitations of VLAN ID, MAC address tables and BRAS sessions. Following simple rules such as creating Ethernet VLAN islands, the access provider can deploy a scalable solution for residential services. A highly scalable and efficient deployment for Ethernet can further be obtained by using VPLS or VPWS solutions, especially when the network provider also wants to offer its customers Ethernet business services, such as E-LAN and E-LINE services.

This paper has further shown that optimized delivery and efficient support of multimedia services in the access network require an increase of service awareness and subscriber intelligence in the access network. Concretely, this increase is seen through the need for service and subscriber-oriented functions, called service enablers, on the access node. These service enablers either increase the subscriber intelligence in the DSLAM, such as the DHCP relay and the 802.1X authenticator, or increase the service awareness, such as the multicast enabler and the QoS enablers. Further deployment of multimedia services in broadband access will require new service enablers to be implemented in the access network.

In fact, this subscriber and service intelligence is more naturally implemented in packet-based access solutions, because it requires the analysis of Ethernet frames and IP packets in the access node.

Alcatel is ready to face the challenge brought on by these new developments. To meet the requirements of this new network environment, the Alcatel product portfolio and the feature set of each specific product is continuously evolving. Several steps have been taken towards the evolution of the access product range and the development of new product lines towards full-service packet-based DSLAMs and access multiplexers. Alcatel also provides Ethernet aggregation and service edge devices, thereby offering a comprehensive multi-service Ethernet broadband access solution.

Alcatel platforms will continue to evolve towards even more service and subscriber awareness and, in connection with that, towards more IP intelligence.

References

[1] "Information technology — Telecommunications and information exchange between systems — Local and metropolitan area networks — Common specifications — Part 3: Media Access Control (MAC) Bridges", IEEE 802.1D, Draft 1.4, 2003;

[2] "IEEE Standard for local and metropolitan area networks – Virtual Bridged Local Area Networks," IEEE 802.1Q, 1998;

[3] "Virtual Bridged Local Area Networks – Amendment 4: Provider Bridges", IEEE 802.1ad, Draft 1.4, 2003;

[4] L. Mamakos et al. " A Method for Transmitting PPP Over Ethernet (PPPoE)", Internet Engineering Task Force, IETF RFC 2516, February 1999.

[5] W. Simpson, "The Point-to-Point Protocol (PPP)," STD 51, Internet Engineering Task Force, IETF RFC 1661, Jul. 1994;

[6] Sven Ooghe, Erwin Six " New Service Architectures for DSL Networks", Alcatel Technology white paper, November 2003.

[7] M. Patrick. DHCP Relay Agent Information Option, Internet Engineering task force, IETF RCF 3046, January 2001.

[8] "IEEE Standard for local and metropolitan area networks - Port-Based Network Access Control," IEEE 802.1X, 2001;

[9] Jerome Moisand et al.," Use of DHCP Relay Agents and PPPoE Intermediate Agents for DSL line identification In Ethernet-based access networks" DSL Forum contribution dsl2004.071, March 2004.

[10] http://portal.etsi.org/tispan/TISPAN_ToR.asp

[11] R Droms et al.,"RADIUS Attributes Sub-option for the DHCP Relay Agent Information Option", Internet Engineering Task Force, draft-ietf-dhc-agentopt-radius-07.txt, July 2004.

[12] DSL Forum TR-069 CPE WAN management protocol, 2004

[13] "Media Access Control Parameters, Physical Layers and Management Parameters for subscriber access networks", IEEE Std 802.3ah-2004

[14] http://www.ist-muse.org

ALCATEL 12 >

Abbreviations

AAA Authentication, Authorization & Accounting
AAL5 ATM Adaptation Layer 5
APAC Asia – Pacific
ARP Address Resolution Protocol
ASP Application Service Provider
ATM Asynchronous Transfer Mode
BRAS Broadband Remote Access Server
CAPEX Capital Expenditure
CoS Class of Service
CPE Customer Premises Equipment
C-VLAN Customer VLAN
DDoS Distributed Denial of Service
DHCP Dynamic Host Configuration Protocol
Diffserv Differentiated services
DoS Denial of Service
DSL Digital Subscriber Line
DSLAM DSL Access Multiplexer
DVD Digital Versatile Disk
EAP Extensible Authentication Protocol
EFM Ethernet in the First Mile
E-LSP Experimental bits inferred Label Switched Path
GigE Gigabit Ethernet
HSIA High-Speed Internet Access
IGMP Internet Group Management Protocol
IMS IP Multimedia Subsystem
IP Internet Protocol
ISP Internet Service Provider
LAN Local Area Network
MEF Metro Ethernet Forum
MPLS Multi Protocol Label Switching
MSTP Multiple Spanning Tree Protocol
NGN Next Generation Network
NSP Network Service Provider
OAM Operation, Administration & Maintenance
PPP Point-to-Point Protocol
PPPoA PPP over ATM
PPPoE PPP over Ethernet
PVC Permanent Virtual Circuit
QoS Quality of Service
RADIUS Remote Authentication Dial In User Service
RED Random Early Discard
RG Residential Gateway
RSTP Rapid Spanning Tree Protocol
SIP Session Initiation Protocol
SME Small & Medium-sized Enterprise
SOHO Small Office/Home Office
STP Spanning Tree Protocol
S-VLAN Service VLAN
ToS Type of Service
TV Television
UBR Unspecified Bit Rate
VB Virtual Bridge
VLAN Virtual LAN
VOD Video On Demand
VPLS Virtual Private LAN Service
VPWS Virtual Private Wire Service
3GPP 3rd Generation Partnership Project

Jeanne De Jaegher received a PhD in theoretical physics from the Katholieke Universiteit Leuven in 2000. She is expert research engineer in network architectures for broadband access and metro networks in Alcatel's R&I division. In the last two years she has been heavily involved in the development of new packet-based solutions for access networks. She is also sub-project leader of a European IST FP6 Integrated Project called MUSE (Multi-Service Access Everywhere).

Piet Vandaele received an electrical engineering degree and a Ph.D. in applied sciences from the Katholieke Universiteit Leuven (KUL), Belgium, in 1995 and 1999, respectively. In 2000, he joined Alcatel's DSL Research & Innovation group in Antwerp. He is currently a Network Analyst working on future DSL access architectures in the Alcatel Corporate Network Strategy Group in Antwerp, Belgium.

Dominique Chantrain is product manager in the Alcatel DSL product group, focusing on the Ethernet & IP features of the Alcatel DSLAM product portfolio. She received an M.Sc. degree in electrical engineering from the Katholieke Universiteit Leuven (KUL), Belgium, in 1991. She then joined Alcatel, initially working as a software engineer, but soon making the step towards systems and network design. For over five years, her activities have focused on network architectures and services for IP/Ethernet access networks.

Davy Damien is a Network Analyst working on DSL data networks architectures in the Alcatel E&S support center in Antwerp, Belgium. Damien graduated in 1987 from "groupe des Ecoles Centrales" one of the leading French engineering schools. He also has a diploma in accounting techniques from IMD in France. He joined Alcatel in 1988, starting his carrier in datacom networks for enterprises and completing the automation and communication networks of a leading factory in USA in 1988 and 1989. In 1994 he was in charge of the sales, marketing, and after-sales department of the optical fiber division (Multimode fibers) before joining the HQ of the Telecom division of the cable group, where he actively contributed to creating joint ventures and investigating major emerging countries. In 1998 he joined Alcatel HQ where he was involved in datacom network partnerships within the operations department. Since 2000, within Alcatel Bell, he has been involved in IP and Ethernet product development and their related market introduction.