

New Service Architectures for DSL Networks

**Making new services plug-and-play thanks to
a DHCP-based IP auto-configuration architecture**

If new services are to enjoy a successful introduction, they must be easy to use. This means that end users should not have to know how to configure and activate the service. This paper addresses how today's DSL access architecture can evolve to support new flexible IP auto-configuration mechanisms. It also introduces a new architecture that no longer makes use of the Point-to-Point Protocol (PPP), as well as describing a number of innovative methods of user authentication and network service provider selection.

With the new service architecture, connectivity establishment is decoupled from data path forwarding, as a result ensuring simplicity and scalability. The architecture uses IP auto-configuration based on the Dynamic Host Configuration Protocol (DHCP) and provides appropriate interworking with evolved AAA and OSS systems.

Using this approach, operators can provide their customers with the broadband service they expect.

Table of Contents

Introduction	1
Today's DSL auto-configuration architecture	1
DSL & ATM auto-configuration	2
IP auto-configuration	2
<i>The Point-to-Point Protocol (PPP)</i>	2
<i>The Dynamic Host Configuration Protocol (DHCP)</i>	3
Evolving the service architecture	3
The Application Service Provider connectivity model	3
The non-PPP access model	4
<i>Architecture benefits</i>	4
<i>IP Auto-configuration</i>	4
DHCP auto-configuration architecture solutions	5
Solutions for network security	5
Solutions for network service selection & user authentication	5
<i>Implicit network service selection/authentication</i>	6
<i>Web portal network service selection/authentication</i>	6
<i>DHCP network service selection/authentication (DHCP proxy)</i>	6
<i>802.1x network service selection/authentication</i>	7
Solutions for session termination	7
Deployment and migration principles	7
Conclusion	8
Abbreviations	8
References	8
Biography	9

New Service Architectures for DSL Networks

Introduction

The number of broadband subscribers has grown at an impressive pace over the last couple of years, thanks largely to the success of high-speed Internet access. This steep growth of broadband subscribers paves the way for a new wave of broadband services that can provide service providers with new sources of revenue.

Migrating to a range of new services beyond high-speed Internet access requires that the transport, management and service architectures evolve accordingly. This is also known as becoming “multi-service-ready” or “triple-play-ready”. One of the key requirements in this evolution is support for a framework that allows the new services delivered to application terminals to be automated, auto-configured, and managed.

This paper addresses the evolution of the service architecture.

First, it describes the current service architecture used for high-speed Internet access. Then it introduces a new service architecture that targets unified support for various new services.

The Internet Protocol (IP) is rapidly becoming the unified network layer for new network services such as Voice over IP (VoIP) or Video on Demand (VoD). Consequently, new applications are increasingly being offered in an architecture that no longer makes use of the Point-to-Point Protocol (PPP). An advanced IP auto-configuration solution and associated management, Authentication, Authorization, and Accounting (AAA), and Operation Support Systems (OSS) infrastructure accompany this evolved architecture. This paper introduces a number of innovative methods that enable user authentication and network service provider selection. It also shows how these methods can interwork with the IP auto-configuration process based on the Dynamic Host Configuration Protocol (DHCP).

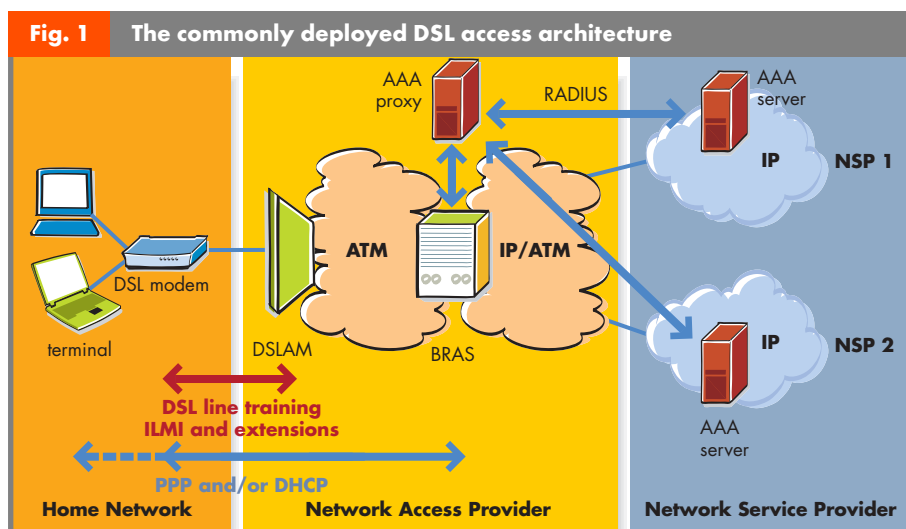
With the evolution of the service architecture comes a need for an appropriate migration strategy for service providers. In the last section, this paper gives a preview of how to ensure smooth migration and thereby guarantee that the approach does not disrupt existing services.

By ensuring that the network can support the features described above, service providers can make the DSL access network truly “triple-play-ready”. With its powerful and extensive access product portfolio, Alcatel is committed to supporting evolution to the new service architecture.

Today’s DSL auto-configuration architecture

The goal of auto-configuration is to minimize, or even eliminate, the effort required by the user to configure the Customer Premise Equipment (CPE), but without merely shifting the burden to the operator. This is achieved by developing network mechanisms to automate initial configuration and life-cycle management of the CPE. This lowers the barrier for users to adopt new services, since user knowledge and interaction related to service activation is minimized. Furthermore, it reduces the provisioning time, meaning that services are activated much faster.

Figure 1 gives an overview of the currently deployed DSL access architecture and associated auto-configuration building blocks required to provide wide area network (WAN) connectivity management for high speed Internet access. A distinction is made between two business roles. The Network



Access Provider (NAP) delivers DSL access network services and connectivity to one or more Network Service Providers (NSPs). The Network Service Provider (NSP) includes both Internet service providers (ISP) and corporate networks. It provides addressing and connectivity to an Internet Protocol (IP) network.

In this architecture, the Broadband Remote Access Server (BRAS) plays an important role in the entire service connectivity/delivery process. It is involved in the IP auto-configuration process, linking to the Authentication, Authorization, and Accounting (AAA) infrastructure of the NAP and the NSPs and providing connectivity to the desired NSP.

The auto-configuration process is centered around the user terminal and/or DSL modem (jointly called the CPE). When the CPE is activated, it retrieves knowledge from the network incrementally until the service can be activated. The auto-

New Service Architectures for DSL Networks

configuration process can therefore be regarded as a “bootstrap” process, whereby the terminals are gradually configured at each layer of the communication stack.

DSL & ATM auto-configuration

The first step of the auto-configuration process is the activation of the DSL line. Physical connectivity between the DSL modem and the DSL access multiplexer (DSLAM) is established when the DSL modem is activated; the modem can determine the achievable DSL bit rate using a training mechanism.

Once the DSL line is active, ATM auto-configuration may be performed. In today’s DSL architectures, the NAP uses primarily ATM permanent virtual connections (PVCs) to establish connectivity between the DSL modem and the BRAS. If the PVC(s) have not been pre-configured in the DSL modem, it may identify the provisioned PVCs using the Integrated Local Management Interface (ILMI) protocol [1]. ILMI runs between the DSL modem and the DSLAM and provides a full description of the configured PVC(s). It provides the DSL modem with all the necessary information to fully describe the PVC, including the virtual path identifier (VPI), the virtual circuit identifier (VCI), and the type of ATM adaptation layer (AAL) used by the PVC. In addition, the ILMI can be used to pass information on the type of protocol encapsulation used by the PVC to the DSL modem. This is described in DSL Forum TR-037 [2].

IP auto-configuration

The network layer can be activated using the ATM connectivity to the BRAS. IP connectivity needs to be established when DSL is used for high-speed Internet access. This results in the configuration of all network parameters in the CPE, including its assigned IP address and the IP addresses of various servers, such as the domain name system (DNS) servers.

Typically, IP auto-configuration will be combined with network service selection and user authentication to control access to the user’s preferred NSP. For example, a user could dynamically select the desired ISP for high speed Internet access when connection is established. Therefore, IP auto-configuration is closely aligned with the AAA infrastructure of both the NAP and the NSPs. Authentication and Authorization will verify whether or not the user is allowed connection to a certain NSP. Accounting will make time and volume information available to the NSP to bill the user.

Depending on the capabilities of the DSL modem, IP auto-configuration for broadband services takes place at the user terminal or at the modem itself.

- If a bridged DSL modem is used, IP auto-configuration will be performed at the terminals; the modem will simply bridge Ethernet frames, without being aware of the network layer protocols and without having to worry about IP configuration.

- If a routed DSL modem is used, the modem has the intelligence to initiate IP auto-configuration itself. Terminals behind the modem may then use DHCP for local IP address assignment inside the LAN.

The protocols used for IP auto-configuration are the Point-to-Point Protocol (PPP) and the Dynamic Host Configuration Protocol (DHCP). Their use in DSL access is described in DSL Forum TR-044 [3].

The Point-to-Point Protocol (PPP)

Currently, residential high-speed Internet access predominantly uses PPP to configure basic IP connectivity [4]. The first major deployment of PPP was to provide narrowband Internet connectivity over PSTN access networks. In the move from a narrowband to a broadband architecture, PPP migration ensured that the user authentication and network service selection infrastructure was reusable. PPP allows the transport of network layer packets between two peers. In DSL access networks the peers are typically a PC or DSL modem and a BRAS. Different architecture variants exist depending on which business role (NAP or NSP) is controlling the BRAS. Figure 1 shows the case where the BRAS is controlled by the NAP. In this case PPP sessions may be terminated in the BRAS and IP packets forwarded to the appropriate NSP(s). The BRAS of the NAP could also simply relay the PPP sessions towards the NSP using a tunneling mechanism. This is commonly performed using the Layer 2 Tunneling Protocol (L2TP). In this case, an L2TP tunnel is established between an L2TP Access Concentrator (LAC) in the Access Network (i.e., a BRAS is acting as a LAC) and an L2TP Network Server (LNS) in the NSP network (i.e., a BRAS acting as an LNS).

Using the Link Control Protocol (LCP), PPP negotiates configuration options specific to the data link layer for connecting the modem and the BRAS. LCP is also used to keep the PPP session alive through a periodic polling mechanism between the peers. When a connection is made, users can prove their identity using an Authentication Protocol, such as the Password Authentication Protocol (PAP) or Challenge Handshake Authentication Protocol (CHAP). This mechanism may also be used to select the network service by adding the desired NSP to the username. For example, johndoe@isp1.com indicates that user johndoe would like to connect to service provider isp1.com¹. The BRAS will verify that the user is authenticated and authorized to establish a connection to the requested NSP. Typically this involves a process whereby the BRAS contacts the NAP’s AAA proxy, which will contact the AAA server of the requested NSP. This may be done using, for example, the Remote Authentication Dial-In User Service (RADIUS) [5]. After user authentication, a Network Control Protocol (NCP) is used to establish network layer connectivity. For Internet access the IP Control Protocol (IPCP) is used.

¹ This syntax is known as a “Network Access Identifier” (NAI)

New Service Architectures for DSL Networks

The PPP connectivity model requires various stateful control protocols to be tied to the data path operation. Specifically, once PPP connectivity is successfully established, the PPP process will remain active in the PC or DSL modem and the BRAS for the entire duration of the session. For new broadband services, this may prove to be a disadvantage, since it needlessly increases architecture complexity.

The Dynamic Host Configuration Protocol (DHCP)

DHCP is a discovery and configuration protocol initially targeted towards use in LANs [6]. It uses a DHCP client on the CPE that tries to contact a DHCP server in the network using a discovery mechanism. DHCP provides an extensive set of IP configuration parameters, allowing full configuration of the IP layer of the user terminal. Additionally, it allows configuration of information related to the services offered over the IP network, such as the names of Session Initiation Protocol (SIP) servers or video servers. Because DHCP was primarily designed for use in LAN environments, user authentication and network service selection are not inherently supported. Only identification based on the device's media access control (MAC) address is possible.

Although the DHCP server may be embedded in an IP router, it is typically a standalone function. A stateless DHCP relay agent is put in the IP router and relays DHCP messages to the DHCP server. This eliminates the need for a DHCP server on each physical network segment and prevents DHCP broadcast packets from entering the NSP network. An additional benefit is the removal of stateful IP auto-configuration operations from the IP router, allowing for a clean split of functionalities.

DHCP is already being used in some residential high-speed Internet access deployments, either to establish IP connectivity or as a complement to PPP to configure those service parameters that are not supported by PPP itself. DHCP is also a commonly used protocol in Public Wireless LANs. The use of DHCP for high-speed Internet access is defined in DSL Forum TR-044 [3].

Evolving the service architecture

Today's PPP-based DSL access architecture is designed effectively to support high-speed Internet access. However, operators are gradually starting to deploy new services over the DSL access infrastructure. This requires the transport, management, and service architectures to evolve accordingly, making the network "multi-service" or "triple-play-enabled". Various standards address some of the aspects that come with this access architecture evolution [7][8][9].

With respect to the service architecture, two key evolution concepts can be identified:

- the notion of a new service provider interconnection model;
- the notion of an IP connectivity establishment model that is no longer based on PPP.

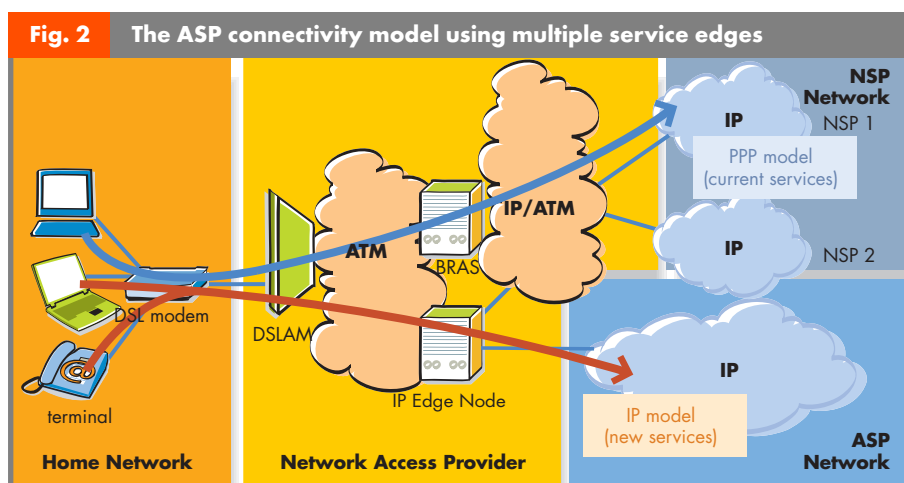
The Application Service Provider connectivity model

As shown in Figure 1, the current connectivity model is based on a connection of multiple NSPs to the NAP. The different NSPs offer various applications in their IP networks. Although this model is ideally suited for high-speed Internet access, it is not necessarily ideal for new broadband services since it lacks network control features that could be required for new services.

A first enhancement to the service architecture to support new broadband services easily is the introduction of a new service provider interconnection model. The new model consists of offering new services using an IP network under the control of the NAP and directly connected to the Access Network. This model is known as the "Application Service Provider (ASP) connectivity model" and is described in TR-058 [7]. The party that performs the role of the NAP will now also perform the role of the NSP, i.e., it hands out IP addresses to subscribers and controls IP connectivity to the ASP network. Different ASPs can use the NAP-provided infrastructure to deliver application or network services to those subscribers. Using this new model, new advanced services such as Video on Demand, Multi-media, gaming, filtered Internet access or access to VPNs via IP-tunneling methods can be offered.

There are two ways of introducing the ASP connectivity model in the currently deployed network:

- a new BRAS deployed in the Access Network can handle both existing and new services as well as the ASP connectivity model. This is the approach taken in DSL Forum TR-059 [8]. The BRAS provides simultaneous connectivity to the different NSP networks as well as the ASP network and can offer a range of IP QoS-enabled



New Service Architectures for DSL Networks

services along side the existing services. This is achieved by controlling congestion in the ATM Access Network;

- the operation of the existing BRAS is left unchanged and an additional service edge (or multiple service edges) is (are) introduced for the new services. This approach is shown in Figure 2. The BRAS provides connectivity to the NSP networks and supports existing services. New services are provided using the ASP connectivity model offered by the new service edge; if desired, the new service edge may also provide connectivity to the NSP networks, albeit using the IP connectivity establishment mechanism described below.

There are a number of benefits in deploying multiple dedicated service edges:

- **Availability:** by separating traffic onto different nodes engineered to different standards, risk is diversified. High availability traffic (e.g., VoIP) does not share nodes such as a BRAS with best-effort Internet traffic;
- **Design effectiveness:** each service edge can be built to optimally manage the trade-off between functionality and complexity for the set of services it carries. There is no need to provide 99.999% availability on a platform used for Internet traffic just because it also needs to handle voice traffic;
- **Security:** each service edge can enforce security policy that is relevant to the set of services it carries. For example, a Voice Gateway can filter out all traffic that is not SIP or H.323-based.

Additionally, it will be shown in the next sections that the use of a separate IP Edge Node allows the IP connectivity establishment mechanism to evolve without impacting the currently deployed PPP approach.

The non-PPP access model

A second enhancement to the service architecture is the introduction of the non-PPP access model. While today's high-speed Internet access architecture is centered around the use of PPP, new services offered with a range of new terminals use a pure IP — or “non-PPP” — approach instead. For instance, IP phones and Set-Top Boxes used to offer new services over DSL to TV sets no longer use the PPP protocol to establish connectivity to the service provider. In a non-PPP architecture, IP packets are directly transported over the layer 2 network between the CPE and the IP Edge Node².

Architecture benefits

By moving to a non-PPP architecture, a number of architecture benefits are obtained:

- The data plane operation is considerably simplified, since there is no longer any need to terminate PPP sessions in the terminal, DSL modem, and BRAS. The data plane operation

(i.e., IP forwarding) can be fully separated from control plane operation (i.e., handling the IP control protocols). Furthermore, by introducing a DHCP relay agent in the IP Edge Node, it is even possible to remove stateful IP auto-configuration out of the IP Edge Node altogether;

- The approach allows subscribers to use the same auto-configuration process for new terminals, independently of the type of DSL modem:
 - In the case of a bridged modem, the DHCP messages originating from the terminals will be sent transparently through the DSL modem (much like the PPPoE messages are transparently sent to the BRAS as well);
 - In the case of a routed modem, the DHCP messages will be processed by the modem. The modem either contains a DHCP relay agent or acts as a combined LAN-side DHCP server + WAN-side DHCP client. In the latter approach, the modem can separate the IP address assignment process in the LAN from that of the WAN.
- The approach allows advanced access network features such as QoS and multicast to be supported. Contrary to a non-PPP architecture, the connection-oriented nature of PPP implies that the stream of IP packets leaving the PPP connection must be the same as the stream of IP packets entering the PPP connection. Similarly, PPP prevents the insertion of new packets in the PPP connection somewhere between the peers. This implies that the non-PPP architecture has to be used if the underlying network features need to be supported. This could be the case when performing multicast traffic replication in an ATM or Ethernet switch, or when configuring ATM or Ethernet QoS in the Access Network.

The non-PPP access model can be used in both variants that enable the introduction the ASP connectivity model. In case a second service edge is introduced, existing services are inherently not impacted, since all BRAS-based services can keep using the PPP model; new services can be directed towards the IP Edge Node, which will no longer make use of the PPP connectivity model. Although it is less compelling to evolve the access model in case of a single edge network architecture, the benefits of a non-PPP architecture are equally valid.

IP Auto-configuration

One of the key requirements when moving from a PPP-based DSL access architecture to a non-PPP architecture is to ensure that the accompanying IP auto-configuration architecture has evolved accordingly. First of all, DHCP clients instead of PPP clients will be deployed at the terminal and/or modem. Given the trend to introduce more non-PC terminals in the home, it is expected that DHCP will play an increasingly important role in future IP auto-configuration architectures.

Since DHCP processing only occurs at session establishment time or at the occasional renewal of the IP address lease (e.g., once every 20 minutes), processing requirements are significantly smaller.

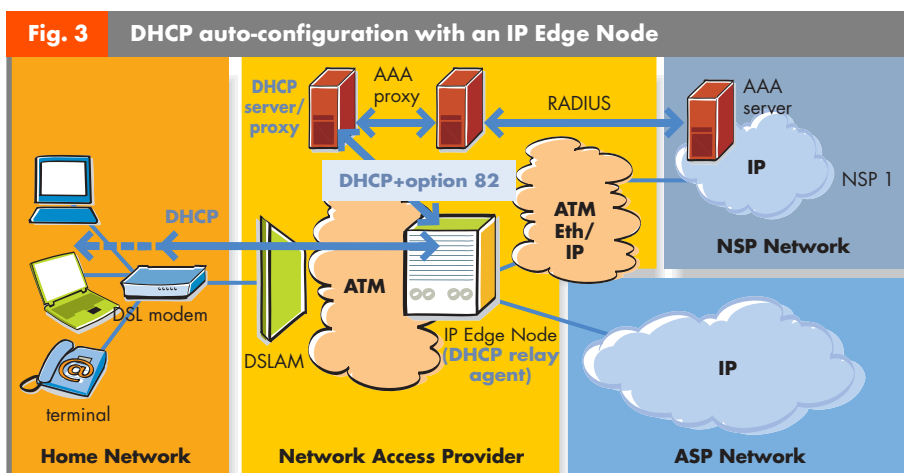
² In this paper, the terms “BRAS” and “IP Edge Node” are used to indicate a network element performing IP forwarding and supporting PPP (i.e., PPP termination) and DHCP (i.e., DHCP relay agent or DHCP server), respectively.

New Service Architectures for DSL Networks

Due to the layered design of the auto-configuration architecture, the new IP auto-configuration architecture is compatible with ILMI auto-configuration. This has the benefit that the value of these mechanisms can be reused when migrating away from PPP. This is especially true since multi-service access architectures may provide connectivity to multiple service edges that are specifically designed to support the new services, resulting in the use of more than one ATM PVC per subscriber. Similarly, the introduction of ATM QoS may result in an increased number of PVCs per subscriber. For instance, one PVC supporting best-effort traffic could connect to a BRAS for high-speed Internet access, while another PVC supporting real-time traffic could be used simultaneously to connect to a Video-on-Demand server.

DHCP auto-configuration architecture solutions

Figure 3 shows the different network elements and protocol interactions involved in the DHCP-based IP auto-configuration process. The BRAS is not shown in this figure, since it provides PPP connectivity to NSPs. As such, this is not relevant to this section. The architecture is built on the following functions:



- A DHCP client in the terminal and/or DSL modem;
- A DHCP relay agent in the IP Edge Node or in the DSLAM for security;
- A stand-alone DHCP server or DHCP proxy interfacing with the AAA infrastructure;
- The existing AAA and Operation Support Systems (OSS) infrastructure.

Moving away from PPP implies that some features of the PPP architecture are no longer available. This means new solutions need to be sought to provide network security, network service selection (in case of NSP connectivity), and user authentication. Currently there is no unique or standardized non-PPP architecture. This section proposes a number of innovative solutions that meet these goals and shows for which services they are applicable.

Solutions for network security

To enable IP connectivity establishment, the IP Edge Node will process DHCP packets using either a built-in DHCP server or a DHCP relay agent. The IP Edge Node will also need to perform a number of functions that provide network security, such as installing filters that prevent malicious packets from entering the network (e.g., packets with a different source IP address than the one assigned by the DHCP server).

To provide an additional level of security when assigning IP addresses, it may be very useful to provide the DHCP server with information on the modem's ATM PVC. The DHCP relay agent in the IP Edge Node can add this information to the relayed DHCP message using the "DHCP relay agent information option" (option 82) [10]. In general, the relay agent can use this option to send identification of the CPE's physical and logical connection to the DHCP server. The relay agent can also send the DHCP server's responses to the correct DHCP client.

Use of a relay agent with option 82 will be especially important for new access architectures based on Ethernet bridging technology. In this case, the DSLAM will no longer use PVCs in the aggregation network but provides access to a shared Ethernet network. A relay agent in the DSLAM can use option 82 to send identification of the DSL port to the DHCP server. This relay agent can be used in combination with "IP spoofing detection", which checks whether the user is authorized to use a specific source MAC address and/or source IP address. This prevents users from faking source IP addresses.

To further improve network security, a message and entity authentication mechanism based on shared secrets could be used [11]. Unfortunately, this mechanism does not provide a flexible network service selection mechanism, nor does it allow easy integration with the NSPs AAA infrastructure.

Solutions for network service selection & user authentication

Table 1 summarizes the different auto-configuration architectures and shows the new options for network service selection and user authentication. Note that the mechanisms for

	PPP architecture	Non-PPP architecture with DHCP	Non-PPP architecture with 802.1X and DHCP
Network service selection/user auth.	PPP Auth. Protocols + NSP indication in username	Implicit, Web portal or DHCP-based	802.1x-based + layer 2-3 synch.
IP auto-config.	IPCP	DHCP IP parameters	DHCP IP parameters
Service auto-config.	Limited in IPCP (DHCP service parameters)	DHCP service parameters	DHCP service parameters

New Service Architectures for DSL Networks

network service selection are only required in case the non-PPP access architecture is to be used to connect to an NSP. In the case of the ASP interconnection model, service selection will likely not be required, but user authentication may still be used.

In a non-PPP architecture, four different types of network service selection and user authentication can be identified: implicit, Web portal-based, DHCP-based, and 802.1x-based. This section describes these solutions for the general case of combined network service selection and user authentication. This will normally take place in case of NSP connectivity. When a connection to the ASP network is desired, user authentication may still be necessary but network service selection can be omitted, simplifying the approach.

Implicit network service selection/authentication

A first approach to establish IP connectivity to an NSP is to pre-configure the DHCP server with a list of terminal MAC addresses to be associated with a specific IP Edge Node, used for a specific service. This can, for example, be used for an IP phone connecting to a specific Voice over IP service provider. Authentication is based on the device's MAC address. The approach can be combined with the use of a relay agent and option 82. In this case, service selection is based on the use of a different logical connection (e.g., a different ATM PVC) for that service.

This mechanism does not require new protocols or extensions of existing protocols. The approach may be part of the service provider's migration strategy: by introducing a new IP Edge Node, the existing high-speed Internet access service can be kept unchanged, while new services are offered using the non-PPP architecture and DHCP to the IP Edge Node. On the other hand, the approach is not very flexible.

Web portal network service selection/authentication

To allow for a greater level of dynamism, a Web portal can be introduced to provide the required user authentication and network service selection features using the Hyper Text Transfer Protocol (HTTP).

When the user terminal establishes IP connectivity, it first obtains an IP address located inside an isolated address realm, which offers limited communication possibilities. Additionally, the DHCP server may provide the client with the IP address of the Web portal, which is also located inside this address realm. This avoids the user's having to configure the Web portal's IP address himself.

Using the temporary IP connectivity, the user contacts the Web portal, where he is able to select the desired NSP and provide the required credentials using a Web form. The information is sent to the Web portal, which contacts the NSP's AAA infrastructure to authenticate the user.

On successful authentication, the Web portal notifies the DHCP relay or server of the selected NSP. The DHCP client contacts the DHCP server to initiate a reconfiguration of the IP parameters. This can happen in two ways:

- A DHCP protocol extension, known as the DHCP FORCERENEW message can be used by the DHCP server to force the DHCP client into the DHCP RENEW state [12].

The client will then start the reconfiguration process. This approach is very fast, but requires client and server to support the extension;

- The lease time associated with the temporary IP address is set to a low value (e.g., 10-30 seconds). The resulting periodic timeouts will also put the DHCP client in the RENEW state. During network service selection and user authentication, connectivity to the isolated IP address realm is kept. After successful authentication, IP parameter reconfiguration can take place when the lease timer has expired. This approach is compatible with existing clients, but introduces a small delay between network service selection and IP connectivity establishment.

Web portal-based network service selection is an elegant solution for PCs but may not be applicable to terminals that do not provide Web portal communication (e.g., IP phones).

DHCP network service selection/authentication (DHCP proxy)

Network service selection can also be done with the DHCP protocol itself. DHCP provides a mechanism for the client to request a specific network configuration based on its "**User Class**" (option 77). This mechanism is sometimes used in enterprise networks to allow terminals to advertise the department to which they belong. The option can be reused in a DSL access environment to support network service selection. The User Class would then contain the username, the desired NSP, and the user's credentials. The syntax of this option could be similar to that of PPP network service selection, e.g., `johndoe@isp.com:password`.

If it is undesirable to send the password in cleartext, a new mechanism can be used where the DHCP client adds a message authentication code, calculated based on the DHCP message transaction ID (a random number chosen by the client) and the user password. Combined with the use of the User Class option, this provides flexible network service selection, message, and user authentication, while supporting interworking with the NSP's AAA infrastructure. The NAP does not necessarily need to know the user's password and can rely on the NSP to perform the AAA process. The mechanism is similar to CHAP, although the "nonce" value³ is generated by the client instead of the server. This can be combined with the additional message and entity authentication mechanism defined in [11] to support mutual authentication.

Figure 3 shows the architecture with the functions required for DHCP network service selection. When adding user authentication and network service selection mechanisms to DHCP, a protocol interaction with the AAA infrastructure becomes necessary. This is achieved using a so-called "DHCP proxy". This function combines the role of a DHCP server with an AAA (e.g., RADIUS) client that interacts with the AAA server of the desired NSP (possibly indirectly using the AAA proxy of the NAP).

³ "Nonce" stands for "no more than once" and indicates an automatically generated unique number used for security applications.

New Service Architectures for DSL Networks

On reception of a DHCP DISCOVER message, the DHCP proxy extracts the information in the message to create a RADIUS message. Specifically, the information in the User Class option will be used when filling in the RADIUS User-Name and User-Password attributes. The DHCP proxy then initiates a RADIUS authentication message exchange with the AAA proxy or the desired NSP AAA server. As with PPP-based IP connectivity establishment, RADIUS can be used to communicate basic IP configuration parameters to the NAP. DHCP could be used to communicate additional advanced IP configuration parameters to the NAP.

As with the position of the DHCP server, the DHCP proxy could either be implemented in the IP Edge Node or could be a standalone function that interfaces with the network for connectivity control and accounting purposes.

DHCP-based network service selection could be used for user terminals that do not have access to a Web portal, such as IP phones or STBs.

802.1x network service selection/authentication

An emerging authentication mechanism for clients connecting to an IEEE 802 network such as Ethernet (access) networks and 802.11 (public) wireless LANs is IEEE 802.1x [13]. The standard 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. The Authenticator controls the operational state of its controlled ports based on the outcome of the authentication process. The standard allows the Authenticator to relay EAP messages between the Supplicant and an Authentication Server, using, for example, RADIUS. This results in a model that looks like the AAA communication infrastructure described previously.

The 802.1x mechanism could be used for user authentication and network service selection in a DSL access architecture. The Authenticator would then need to be located in the DSLAM connected to an Ethernet network; the Supplicant could either be located in the terminal or in the DSL modem. In the specific case of a bridged modem, care is needed to ensure that the EAP messages sent by the Supplicant in the terminal reach the Authentication in the DSLAM. The 802.1x standard does not allow for authentication between indirectly connected peers. Therefore, appropriate interworking is required in the bridged modem.

The 802.1x process needs to be synchronized with the IP auto-configuration process. One approach uses 802.1x to provide authenticated access to a specific sub-network in the Ethernet network, e.g., a specific virtual LAN (VLAN) depending on the desired NSP. This can be seen as a form of "layer 2 service selection". Once connectivity to the VLAN is established, the normal IP auto-configuration procedures can be used to establish IP connectivity.

Another approach uses 802.1x to provide authenticated access to the layer 2 network, but does not use dedicated VLANs for different NSPs. Synchronization can be done by

means of interaction between the Authenticator and the DHCP relay agent, provided that both reside in the same network element (e.g., DSLAM). On successful authentication, the Authentication Server provides the Authenticator with a number of parameters that can be used to identify the NSP service. When the DHCP client initiates IP auto-configuration, the DHCP relay adds these parameters to the relayed message. This allows the DHCP server to send the appropriate IP configuration parameters to the DHCP client.

Solutions for session termination

In a PPP architecture, a user will normally terminate the session by sending an IPCP Terminate message. Otherwise, the LCP periodic polling mechanism can detect whether the PPP session has terminated, at which point the IP address assigned to the CPE can be put back in the pool of available IP addresses.

A DHCP server expects a DHCP RELEASE message to correctly end a DHCP session. When the session is not closed properly, the DHCP sever may also use a timeout mechanism. However, typical lease times of an IP address are much higher (order of hours) than the PPP LCP timeout mechanism (30 seconds to two minutes). This may be too rough a resolution for security and accounting reasons.

By increasing the resolution of the DHCP timeout mechanism to something like one to 10 minutes, a good balance between processing requirements at the DHCP server, security, and consumption of IP addresses in the IP address pool can be achieved. This is sufficient for accounting based on traffic volume; accounting based on service time could still be done on a per application basis (e.g., time-based accounting for a Voice over IP call).

Deployment and migration principles

The introduction of new services may also require changes beyond the service architecture; the evolution of the access network from a transmission technology viewpoint should also be taken into account. As described in [14], ATM, Ethernet, and subtending technologies can play a significant role in reducing residential service costs through aggregation in the second mile. The key consideration for a service provider is the choice of an appropriate mix of technologies to best meet its business objectives. This section briefly highlights how the migration towards new service architectures ties into the evolution to other aggregation technologies.

First of all, when deploying the service architecture in an ATM access network, the evolution does not impact the Access Node or ATM switches; both can continue to operate as before. If desired, new features such as QoS using multiple VCs or IGMP snooping with ATM point-to-multipoint VCs can be offered if required for advanced services. The non-PPP IP auto-configuration architecture does introduce some changes to the BRAS or IP Edge Node. A first approach could be to add the described DHCP features to the BRAS itself. As an alternative approach, the new DHCP features could be offered by new and dedicated service platforms such as an IP Edge Node. With the

New Service Architectures for DSL Networks

second approach, it is possible to ensure a non-disruptive approach for existing services, while at the same time offering new services on a new platform. Additionally, it allows some traffic to be offloaded from the BRAS to a separate IP Edge Node.

In case the service architecture is tied to the use of an Ethernet access network, some additional deployment considerations should be taken into account. Since the Ethernet paradigm creates a broadcast domain in the access network, security needs to be considered. This includes avoiding IP spoofing as well as a range of denial-of-service attacks. Security can be ensured by placing specific relay features in the Access Node; a DHCP relay can be used to shield DHCP protocol message from other subscribers as well as to enable the Access Node to perform IP spoofing detection. Similarly, relay features may also be present for other protocols such as the Address Resolution Protocol (ARP). With these features in place, the non-PPP architecture can operate safely, while at the same time allowing other Ethernet network features such as prioritization to be used.

Finally, as a special case, the Access Node could become an IP node performing IP forwarding. In this case the Access Node acts like an IP Edge Node and may therefore support the same features, such as a DHCP relay or even a DHCP server.

Conclusion

With the evolution to new services beyond high-speed Internet, the transport, management, and service architectures need to evolve accordingly. Many new terminals are no longer using the PPP protocol to establish connectivity to the service provider. Hence, with respect to the service architecture, a paradigm shift from a PPP-centric architecture to a non-PPP broadband access architecture is envisaged, with the Internet Protocol becoming the unified network layer for new network services.

By moving to a non-PPP architecture, data plane operation is considerably simplified and advanced access network features such as QoS and multicast are inherently supported, irrespective of the aggregation technology such as ATM or Ethernet. Furthermore, the approach allows subscribers to use the same auto-configuration process for new terminals, independently of the type of DSL modems. In the non-PPP architecture, the function of a BRAS is gradually replaced by an IP Edge Node.

Accompanying the evolved architecture is an advanced IP auto-configuration solution and associated management, Authentication, Authorization, and Accounting (AAA), and Operation Support Systems (OSS) infrastructure. The new IP auto-configuration architecture will be built around the Dynamic Host Configuration Protocol (DHCP) in combination with new solutions providing network security, network service selection, and user authentication.

The new service architecture provides a suitable migration strategy for service providers. By reusing the existing paradigm for established services and introducing the new

paradigm for new services, a smooth migration can be ensured. Furthermore, the migration towards new service architectures ties into the evolution to other aggregation technologies and can be combined with additional security extensions if required. Alcatel has committed itself to support the evolution to this new service architecture by supporting the required features in its access product portfolio.

Abbreviations

AAA	Authentication, Authorization, and Accounting
AAL	ATM Adaptation Layer
ARP	Address Resolution Protocol
ASP	Application Service Provider
ATM	Asynchronous Transfer Mode
BRAS	Broadband Remote Access Server
CHAP	Challenge Handshake Authentication Protocol
CPE	Customer Premise Equipment
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
DSLAM	DSL Access Multiplexer
EAP	Extensible Authentication Protocol
HTTP	Hyper Text Transfer Protocol
ILMI	Integrated Local Management Interface
IPCP	Internet Protocol Control Protocol
ISP	Internet Service Provider
L2TP	Layer 2 Tunneling Protocol
LAC	L2TP Access Concentrator
LCP	Link Control Protocol
LNS	L2TP Network Server
MAC	Medium Access Control
NAP	Network Access Provider
NCP	Network Control Protocol
NSP	Network Service Provider
OSS	Operation Support Systems
PPP	Point-to-Point Protocol
PAP	Password Authentication Protocol
PVC	Permanent Virtual Connection
RADIUS	Remote Authentication Dial In User Service
SIP	Session Initiation Protocol
VLAN	Virtual Local Area Network
VCI	Virtual Circuit Identifier
VPI	Virtual Path Identifier
VoD	Video on Demand
VoIP	Voice over IP
WAN	Wide Area Network

References

- [1] "Integrated Local Management Interface 4.0," ATM Forum, afilmi-0065.000, Sep. 1996;
- [2] "Auto-Configuration for the Connection Between the DSL Broadband Network Termination (B-NT) and the Network using ATM, (TR-037 update)" DSL Forum Technical Report, TR-062, Nov. 2003;
- [3] "Auto-Configuration for Basic Internet (IP-based) Services," DSL Forum Technical Report, TR-044, Dec. 2001;
- [4] W. Simpson, "The Point-to-Point Protocol (PPP)," STD 51, Internet Engineering Task Force, IETF RFC 1661, Jul. 1994;

New Service Architectures for DSL Networks

- [5] C. Rigney, "Remote Authentication Dial In User Service (RADIUS)," Internet Engineering Task Force, IETF RFC 2865, Jun. 2000;
- [6] R. Droms, "Dynamic Host Configuration Protocol," Internet Engineering Task Force, IETF RFC 2131, Mar. 1997;
- [7] "DSL Evolution - Multi-Service Architecture & Framework Requirements," DSL Forum Technical Report TR-058, September 2003
- [8] "DSL Evolution - Architecture Requirements for the Support of QoS-Enabled IP Services," DSL Forum Technical Report TR-059, September 2003
- [9] "Full-Service VDSL - System Architecture and Customer Premises Equipment", ITU Recommendation H.610, July 2003
- [10] M. Patrick, "DHCP Relay Agent Information Option," Internet Engineering Task Force, IETF RFC 3046, Jan. 2001;
- [11] R. Droms, W. Arbaugh, "Authentication for DHCP Messages," Internet Engineering Task Force, IETF RFC3118, Jun. 2001;
- [12] Y. T'Joens, C. Hublet, P. De Schrijver, "DHCP reconfigure extension," Internet Engineering Task Force, IETF RFC 3203, Dec. 2001;
- [13] "IEEE Standard for local and metropolitan area networks - Port-Based Network Access Control," IEEE 802.1X, 2001;
- [14] M. Crawford, D.Verheye, "Residential Service Aggregation in the Second Mile," Alcatel Telecom Review, Q2 2003, T0306-Second-Mile-EN.pdf, http://aww.alcatel.com/group/cto/tm/atr/public/documents/2003q2/2003q2_10_us.htm



Ooghe Sven

Network Analyst, working on future DSL access architectures. Network Strategy Group, Antwerp, Belgium
Sven Ooghe studied telecommunications networks and computer architectures at the Faculty of Applied Sciences and received an MS degree in computer science from the

University of Ghent (Belgium) in 2000.

In 2000, he joined Alcatel's Network Strategy Group in Antwerp, where he initially worked on Policy Based Networking and Quality of Service in access networks. Currently, he works as a Network Analyst performing research and working on the access strategy. He is also actively involved in standardization, mainly in the DSL Forum. (sven.ooghe@alcatel.be)



Six Erwin

Research Engineer, working on Access & Edge network architectures. Research & Innovation, Antwerp, Belgium
Erwin Six received an MS degree in electro-technical engineering, specialized in telecommunication technology, from the University of Ghent, Belgium in

2001. He joined the Alcatel Research & Innovation (R&I) Center in Antwerp, working as a systems engineer in the access technology group on Gigabit Passive Optical Networks. Presently, he is a member of a joint R&I / Network Strategy Group team which focuses on architectural studies related to Access & Edge network evolution. (erwin.six@alcatel.be)

ARCHITECTS OF AN INTERNET WORLD



Alcatel and the Alcatel logo are registered trademarks of Alcatel. All other trademarks are the property of their respective owners. Alcatel assumes no responsibility for the accuracy of the information presented, which is subject to change without notice.
© 11 2003 Alcatel. All rights reserved. 3GQ 10001 0007 TQZZA Ed.01