



NISCC Technical Note 12/03

18 December 2003

Understanding the Security of ADSL

Key Points

- ADSL services can form part of an appropriately secure solution in the CNI, provided that service providers and customers implement adequate security measures.
- End-to-end security is the key consideration
- PVC based ADSL services may be considered as alternatives to leased line services
- IP based ADSL services do not have a precise circuit switched equivalent
- Separation of ADSL access to critical networks, from internet access, is an important consideration

**National Infrastructure
Security Co-Ordination Centre**
PO Box 832
London, SW1P 1BG

Tel: 020 7821 1330 Ext 4511
Fax: 020 7821 1686
Email: enquiries@niscc.gov.uk
Web: www.niscc.gov.uk

1 Introduction

1.1 Summary of Recommendations

Asynchronous Digital Subscriber Line (ADSL) based services can provide security suitable for many Critical National Infrastructure (CNI) solutions, but it is necessary that the ADSL provider, all downstream operators and service providers, and the end customer follow good security practices. The specific end-to-end solution must be considered, rather than simply the individual components in isolation. Users should undertake a conventional risk assessment procedure as part of any adoption of ADSL technology.

A summary of recommended good practices for services containing an ADSL component is provided below, extracted from a more detailed discussion in section 4 of this paper. If these good practices are followed, then in the context of CNI security, end-to-end Permanent Virtual Circuit (PVC) based services such as BT DataStream are considered broadly equivalent to leased line access to layer 2 services. Because of the Internet-based backhaul of IP-based services such as BT IPStream, these have no simple equivalence with circuit-switched or basic Internet approaches. However with suitable end-to-end countermeasures such as those listed in section 1.2 and 1.3 below, NISCC believes that IPStream is also suitable for many CNI solutions.

1.2 Network Operators/Service Providers Recommendations

At a minimum, shared secret authentication should be implemented between RADIUS clients, proxies and servers, combined with a challenge/handshake authentication protocol that protects passwords from interception. Other authentication mechanisms, such as digital certificates combined with a Public Key Infrastructure (PKI), may offer improved manageability and scalability. (see section 4.7).

Access control should be applied to the Local Area Network (LAN) supporting all authentication servers, so that only legitimate address ranges and necessary protocols can access the servers (see section 4.7).

A single, exclusive service selection should be possible at any one time at the Broadband Access Server (BAS), even when multiple service selections are possible at different times (see section 4.8).

Each service selection should be explicitly permitted by validating the ADSL physical port against the requested service selection in the infrastructure RADIUS (see section 4.8)

ADSL systems used for CNI should not include service selection for basic Internet access (see section 4.8).

Access control should be applied to the Local Area Network (LAN) supporting all L2TP tunnel endpoints, so that only legitimate tunnel addresses and tunnel protocols can access these points (see section 4.9)

Where Layer 2 Tunnelling Protocol (L2TP) tunnels are established across administrative boundaries, authentication of the L2TP tunnel endpoints should be applied (see section 4.9).

Mutual authentication of clients and servers should be applied, and authentication data should be stored and accessed securely, including for management and administrative purposes (see section 4.7)

Split tunnelling presents security issues for remote sites, and should normally be avoided. Customers are advised to check the implementation details of any specific Other Licensed Operators (OLO) IP-VPN to ensure split tunnelling cannot occur in a particular case (see section 4.12).

1.3 Customers/Managed CPE Provider Recommendations

It is essential that the end-to-end solution be considered, rather than simply individual components in isolation. A risk assessment to identify the required security countermeasures for any solution incorporating ADSL should be carried out in the same way as would be required for Internet connectivity.

The security manager should ensure that unauthorised physical or remote access to the ADSL Customer premises equipment (CPE) for Datastream & IPstream services is prevented. It should not be possible to access the ADSL port at the Network Termination point without access controls. It should not be possible to access

the console port of the ADSL equipment locally without access controls, and remote access to the device configuration should be password-protected in line with BS 7799 guidance (see section 4.3)

Users should take care to ensure the physical and technical security of hosts and network ports on the LAN side of an ADSL site (see section 4.5)

Where IPStream is used for CNI systems, IPsec or another approved cryptographic solution should be applied at least between the ADSL CPE and a gateway device within the OLO or corporate network, such that the Internet backhaul portion of the solution is protected (see section 4.10).

User authentication protocols between the ADSL CPE and the downstream OLO or corporate authentication servers should be applied. At a minimum, shared secret authentication should be implemented, combined with a challenge/handshake authentication protocol that protects passwords from interception. Other authentication mechanisms, such as digital certificates combined with a PKI, may offer improved manageability and scalability. (see section 4.11).

2 Overview

2.1 Scope

This technical note is intended to inform and offer advice to readers within government, the CNI and others about the security of networks and services being offered across Digital Subscriber Lines (xDSL). This note concentrates upon ADSL used to access existing Virtual Private Network (VPN) services, including Frame Relay, Asynchronous Transfer Mode (ATM), and Multi-Protocol Label Switching (MPLS)-VPNs, and for direct connection to other company sites. It does not address ADSL for Internet access, or for Internet-based IP-VPNs. Its purpose is to help the NISCC community better understand how ADSL operates, and to suggest security measures that should be considered when ADSL is part of a solution. It is not intended to prescribe or endorse any individual solution.

2.2 Structure

Section 1 is a summary of advice the National Infrastructure Security Co-Ordination Centre (NISCC) offers to customers, service providers and networks operators with respect to making ADSL services reasonably secure. These recommendations are extracted from the longer discussion in section 4 of this paper. Section 2 (this section) gives an overview of the scope and structure of the paper. Section 3 gives a non-technical overview of xDSL and ADSL, and the impact they might have upon remote working. Section 4 gives an overview of the potential security issues associated with ADSL services, and suggests good practice approaches to minimise these. Appendix A gives a more detailed technical description of the BT ADSL implementation, and of how this interconnects with customers and downstream service providers.

3 What is ADSL?

xDSL is a family of technologies that increase the bandwidth available across traditional copper pairs, typically in the access network of incumbent operators. The dominant deployed xDSL technology is ADSL, which offers higher bit rates downstream than upstream. The increased bandwidth of all DSL solutions is achieved by including sophisticated signal processing at each end of the copper pair to overcome the poor transfer characteristic of the basic copper plant. ADSL equipment uses ATM as its layer two protocol, so that in principle multiple services can be provisioned across a DSL link with differing Categories of Service by using multiple ATM virtual circuits.

As users move to ADSL, the increased bandwidth, improved responsiveness, and always-on nature of the service tends to modify how remote access is used, as compared to dial-up modem or Integrated Services Digital Network (ISDN) access. Users with ADSL typically make more use of remote access, and use an increased number of services across it. As a result they are individually more dependent upon the service than are dial-up users. The improved performance of ADSL also means that over time a higher percentage of users will adopt ADSL remote working than has been the case with dial-up access. These factors can present design, configuration and operational challenges to the IT staff and systems in an organisation using ADSL which must be considered, but which are outside the scope of this paper. For example the bandwidth and number of

connections that must be handled by a corporate firewall may increase dramatically as ADSL is adopted for remote access.

ADSL is predominantly used for broadband Internet access today. Low cost services operate at contention ratios of around 50:1, with business services offered at perhaps 5:1 or 10:1. This note does not address the use of ADSL for Internet access. However ADSL will increasingly be used as an access mechanism to layer 2 and layer 3 services, such as MPLS VPNs. This note addresses ADSL used to access these layer 2 and 3 services.

Symmetric Digital Subscriber Line (SDSL) services offer the same data rates upstream and downstream, and can readily be used to offer traditional leased line services by operating with a contention ratio of 1:1, so that the full provisioned bandwidth is available end-to-end. SDSL is expected to be widely available within the next 6-12 months (currently available in limited areas), and is likely to be used to provide virtual leased lines based upon ATM Constant Bit Rate services.

4 Security Aspects

4.1 ADSL physical Layer (DataStream and IPStream)

The physical layer access network in ADSL deployments is the conventional twisted-pair local loop traditionally used for analogue telephony, V series modems or ISDN. The security of this is considered equivalent to that of the local loop used for ISDN or V series modem connection.

4.2 ATM Backhaul (DataStream and IPStream)

ATM PVC services offer no mechanism for endpoint authentication, and so in common with other PVC access mechanisms, physical access to the network termination point and the CPE must be protected. The use of ATM backhaul for ADSL services is considered equivalent to the use of ATM services over leased lines. Because customers have no access to IP layer functionality, these networks are generally considered to have good immunity to attack, and to provide robust separation of traffic on different customer VPNs. Correct configuration of the DSLAM physical ports and VPI/VCI pairs by the access network operator should ensure that traffic cannot be injected into other virtual connections maliciously.

4.3 Security of the xDSL CPE (DataStream and IPStream)

The security manager should ensure that unauthorised physical or remote access to the ADSL Customer premises equipment (CPE) for Datastream & IPstream services is prevented. Countermeasures should be equivalent to those applied to conventional leased line access to Layer 2 services. It should not be possible to access the ADSL port at the Network Termination point without access controls. It should not be possible to access the console port of the ADSL equipment locally without access controls, and remote access to the device configuration should be password-protected in line with BS 7799 guidance. The DataStream service is particularly vulnerable to a CPE-based attack, since no protocol-based authentication is applied. From a CNI perspective, compromise of the DataStream service at another customer's location should not compromise the security of other VPNs, because of the layer 2 separation imposed within the backhaul network. However compromise of a remote location would potentially give access to a complete VPN hence the need for good physical security measures when the DataStream service is used.

4.4 Security of the xDSL CPE (IPStream)

For IPStream-based services, the same vulnerabilities arise as for the DataStream service. It should be assumed that physical access to the ADSL CPE allows authentication passwords to be recovered. In addition to accessing the intended VPN service, someone with access to the ADSL CPE via a console port could potentially alter the configuration of the device so that a different service selection was made, typically to a bogus Internet Service Provider (ISP), from where a range of attacks against the corporate VPN or other VPNs might be mounted.

4.5 Security of the Remote LAN (DataStream and IPStream)

Users should take care to ensure the security of hosts and network ports on the LAN side of an ADSL site. Where access can be gained to hosts or network ports on the LAN side of an ADSL service, the VPN can be

compromised, and a wide range of attacks, including DoS attacks, mounted. Normal precautions to prevent access to the LAN at a remote site should be applied. No specific ADSL issues are believed to exist.

4.6 End-point Authentication between ADSL CPE and BAS (IPStream)

In common with dial-Internet connections, mutual authentication between the Broadband Access Server (BAS) and the client (ADSL modem) is not practical using a shared secret mechanism. This is considered not to present a security issue for CNI use, provided the authentication servers that provide service selection and other customer details (the BT Platform RADIUS servers in this case) are themselves secure. Given the lack of authentication between the CPE and the BAS, it is important that appropriate precautions on service selection and CPE security are applied.

4.7 Protection of Authentication Servers (IPStream)

Denial of Service (DoS) attacks against the authentication services used by IPStream could make the service widely unavailable. Modification of the authentication server data could cause profiles to be unavailable, or bogus L2TP tunnels to be generated.

As a minimum, shared secret authentication should be implemented between RADIUS clients, proxies and servers, combined with a challenge/handshake authentication protocol that protects passwords from interception. Other authentication mechanisms, such as digital certificates combined with PKI, may offer improved manageability and scalability.

Access controls should be applied to the LANs supporting all authentication servers, so that only legitimate address ranges and necessary protocols can access the servers.

Mutual authentication of clients and servers should be applied, and authentication data should be stored and accessed securely, including for management and administrative purposes.

4.8 Service selection within the BT access network (IPStream)

ADSL connections to a BAS in principle allow multiple service selections to be made, and with multiple PVCs operating across the ADSL link, these can operate simultaneously. It is important that control over service selection is applied at the BAS.

A single, exclusive service selection should be possible at any one time at the BAS, even when multiple service selections are possible at different times. This provides some protection against accidental or malicious attacks from one VPN to another, or from the Internet to a VPN via the ADSL CPE.

Each service selection should be explicitly permitted by validating the ADSL physical port against the requested service selection in the platform RADIUS. Restricting the service selection provides some protection against any attack that attempts to connect to a bogus profile by altering the ADSL CPE configuration, and against attacks where a bogus physical port is used to attempt entry to a legitimate service.

ADSL systems used for CNI should not include service selection for basic Internet access; instead profiles should be restricted to those necessary for corporate access. This provides some protection against attacks from the Internet against the CPE, the remote site systems, or the CNI VPN.

4.9 Protection of L2TP tunnel endpoints (IPStream)

Access Control should be applied to the LAN supporting all L2TP tunnel endpoints, so that only legitimate address ranges and ports can access the tunnel endpoints. If tunnel endpoints can be accessed, various attacks, including DoS attacks, can be mounted against the tunnel infrastructure and end user networks.

Where L2TP tunnels are established across administrative boundaries, authentication of the L2TP tunnel endpoints should be applied. Otherwise a bogus L2TP endpoint might establish tunnels in order to mount a DoS or other attack against a tunnel server.

4.10 Security of Internet-based backhaul networks (IPStream)

Where an Internet backbone network is used to transport traffic, it is considered insecure without additional cryptographic countermeasures. L2TP tunnelling can be configured to provide end-point authentication when a control channel is established, but applies no protection to individual tunnels. If tunnel traffic can be accessed, various attacks, including DoS attacks, are possible. The main IETF approach to protecting traffic at the IP layer, carried across an Internet backbone, is the use of IPSec, which can be configured to provide integrity, authentication and confidentiality services on a per-packet basis, as well as replay protection and key management.

Where IPStream is used for CNI systems, IPSec or another approved cryptographic solution should be applied at least between the ADSL CPE and a gateway device within the OLO or corporate network, such that the Internet backhaul portion of the solution is protected. For practical reasons the cryptographic end-points may be within the ADSL site LAN, rather than on the ADSL CPE itself. Cryptographic protection should be applied 'outside' any user authentication protocols carried across the connection, such as PPP-Challenge Handshake Authentication Protocol (CHAP), so that these are also protected. If L2TP is used to support IPSec as a security countermeasure, this is separate to the L2TP transport tunnels used within the IPStream service.

4.11 Authentication of users to downstream service providers and corporate networks (IPStream)

User authentication protocols between the ADSL CPE and the downstream OLO or corporate authentication servers should be applied. At a minimum, shared secret authentication should be implemented, combined with a challenge/handshake authentication protocol that protects passwords from interception. Other authentication mechanisms, such as digital certificates combined with a PKI, may offer improved manageability and scalability.

The same countermeasures applied to protect authentication services within the upstream network should be enforced, i.e. mutual authentication of clients and servers should be applied, and authentication data should be stored and accessed securely, including for management and administrative purposes.

4.12 Split tunnelling within downstream OLOs

Split tunnelling presents security issues for remote sites, and should usually be avoided. Provided a single service selection to a corporate network or corporate VPN is permitted at the BAS, split tunnelling cannot occur at the ADSL site. Provided Internet service selection is not permitted, through which an Internet IP-VPN is invoked, then again split tunnelling cannot occur at the ADSL site. However depending upon the downstream service that the ADSL site connects to, split tunnelling may be implemented within a downstream VPN. For example some MPLS-VPN implementations include network-based Internet breakout from/to the VPN, in which case split tunnelling occurs within the downstream OLO service. *Customers are advised to check the implementation details of any specific OLO-IP-VPN to determine whether split tunnelling can occur in a particular case.*

5 Acknowledgements

Thanks are due to BT for permission to extract diagrams from [BT-001] concerning their IPStream architecture for use in this paper.

6 References

[OFT-001]: 'OfTel's Internet and Broadband Brief', dated July 2003, http://www.oftel.org/publications/internet/internet_brief/broad0703.htm

[BT-001]: 'Broadband IP Platform Security White Paper', draft

Appendix A: ADSL Architecture with LLU

ADSL services are usually provided across an existing copper pair owned and managed by the incumbent telecommunications operator. In the UK, this may be BT (nationally, excluding Hull) or Kingston Communications (within Hull). Although cable operators such as ntl and Telewest also own and manage copper pairs to residential customers within their cable franchise areas, they typically adopt other approaches to broadband access such as cable modems.

Local Loop Unbundling (LLU) allows OLOs within the UK to offer broadband services across the BT or Kingston Communications local loop. Unbundling may be logical or physical:

in physical unbundling, an OLO takes over the copper pair between a customer and their local exchange, and provides their own Digital Subscriber Line Access Multiplexor (DSLAM) in BT premises at the copper pair termination point;

in logical unbundling, BT or Kingston Communications install and operate the DSL access network, and sell a wholesale service to OLOs and service providers who wish to offer services to ADSL connected customers. They do this by backhauling the customer traffic to an interconnect point with the OLO who will provide service to the customer;

The logical unbundling approach currently dominates the UK market [OFT-001], with around 99% of ADSL services offered across BT-managed ADSL. Because the majority of ADSL within the UK is offered across BT copper pairs at the moment, this initial technical note focuses upon the BT network and services; please contact NISCC to discuss logical or physical unbundling by other operators or service providers.

The end-to-end architecture of an unbundled service based upon ADSL has four main network components

- The ADSL access circuit, including CPE, the corresponding DSLAM at the local exchange or remote concentration point, and an ATM grooming and aggregation switch
- The backhaul (also known as conveyance by Oftel) from the aggregation switch to an OLO/SP interconnect point. This may be ATM-based, or may use a tunnelling protocol across an IP network as well as, or instead of, the ATM backhaul.
- The OLO/SP network that provides services to the end customer. A wide range of services might be accessed at this point, including Internet, Layer 2 VPNs, and MPLS VPNs.
- The customer network, including other ADSL sites and typically a headquarters site with a higher-speed connection to the OLO service

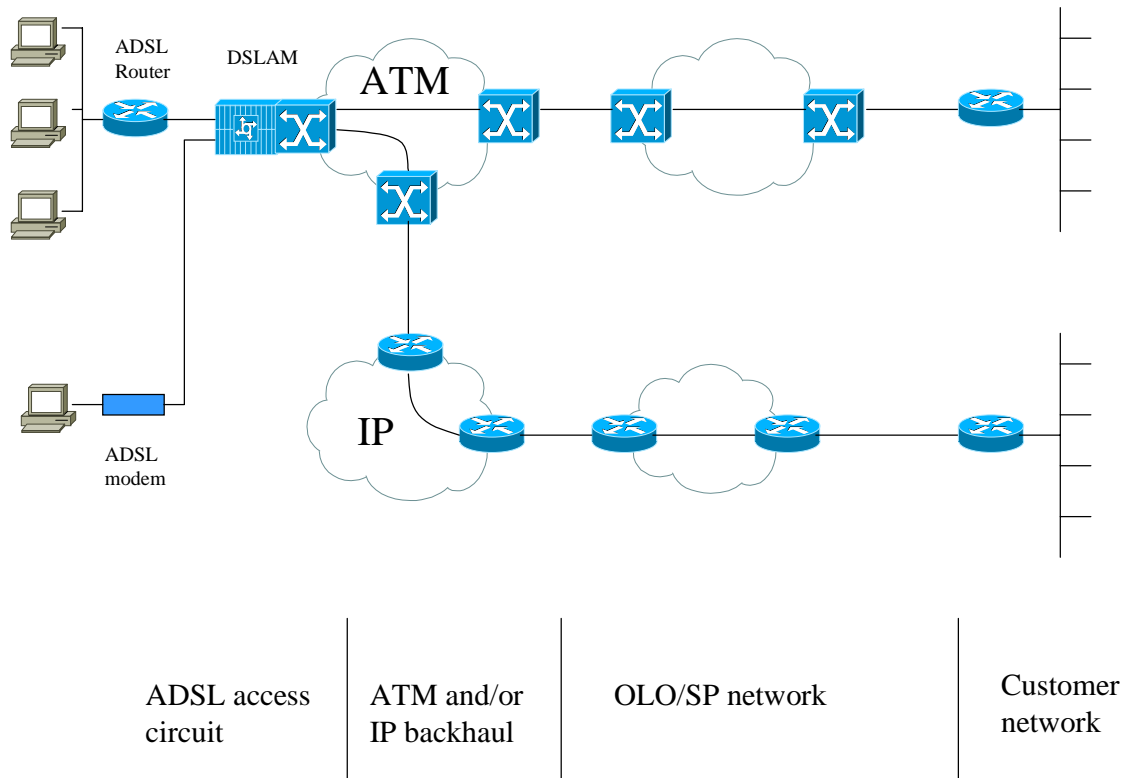


Figure A.1: Overall ADSL architecture with Local Loop Unbundling

7 BT Wholesale ADSL services

7.1 BT Network Infrastructure

The BT wholesale ADSL services offered to OLOs and enterprises in the UK follow the architecture described above. BT DSLAMs are connected across the BT MultiServices Intranet Platform (MSIP) for aggregation of traffic and delivery on to either layer 2 interconnection points with OLOs, or to a BAS at the edge of the BT core IP network.

The MSIP is used to offer native layer 2 services including Frame Relay and ATM, and also provides dial-Internet backhaul to the IP core network, as well as the equivalent ADSL backhaul.

The BT IP core network is assigned Autonomous System number AS 2856, and is called Colossus internally. It is a conventional Internet backbone network, participating in peering with other ISPs, and offering a range of Internet services. AS 2856 is also used to backhaul ADSL traffic which it collects from MSIP nodes to BT's interconnect points with OLOs. As for wholesale dial-Internet traffic, BT uses compelled L2TP tunnels to transport ADSL traffic across the IP backbone.

BT sells wholesale services under the brands DataStream and IPStream. The DataStream product is a pure ATM-based solution, and has no routing functionality. The IPStream product offers various authentication, proxying and configuration features associated with layer 3 networks.

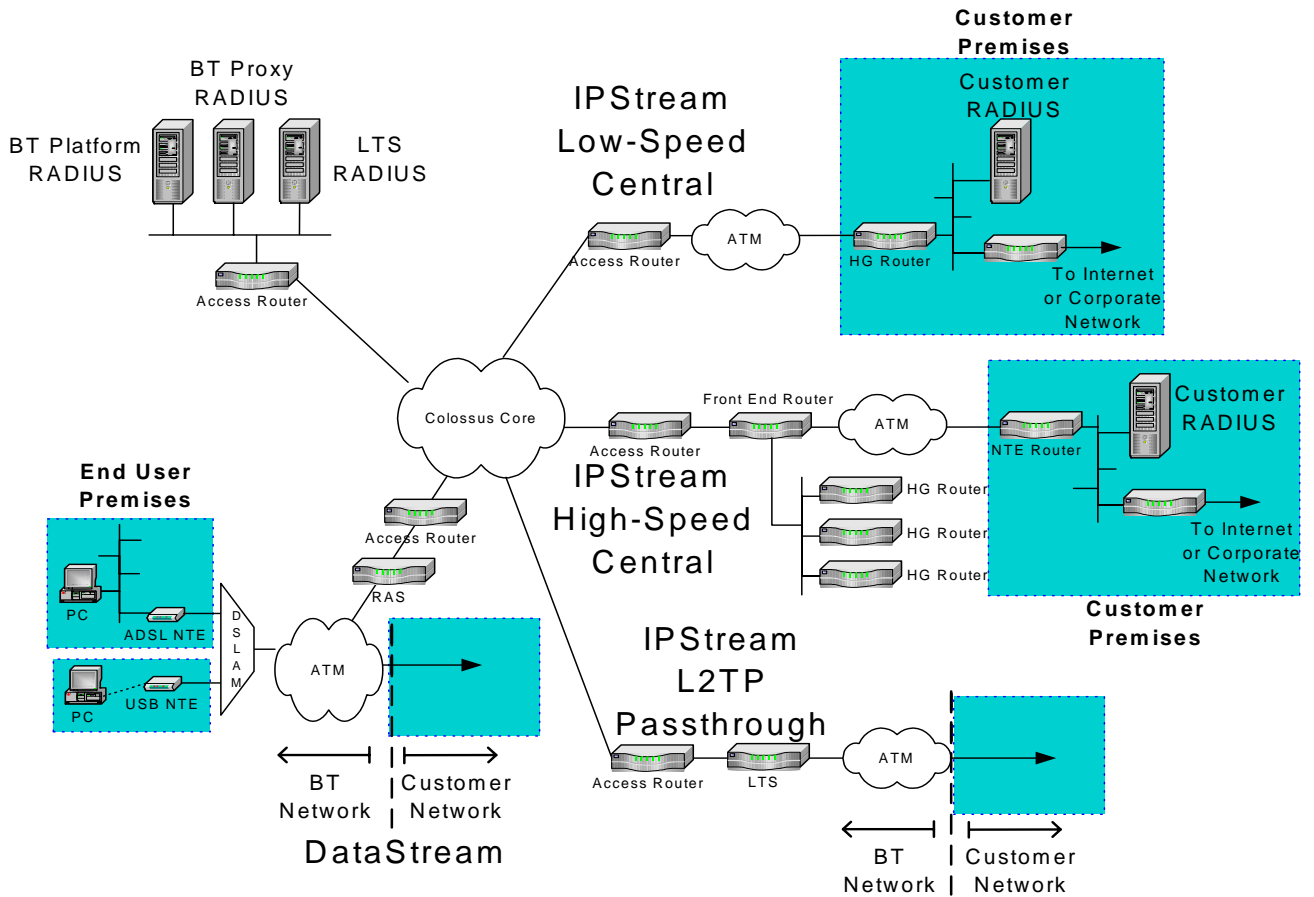


Figure A.2: Overall BT DataStream and IPStream architectures

7.2 DataStream

DataStream provides an ATM PVC service in the access and the backhaul portions of the network. Backhaul is across the BT MSIP, and is implemented exclusively on ATM PVCs. The interconnect to an OLO is also based upon ATM PVCs, carried within a PVP structure for trunking purposes. As for other layer 2 services, any traffic presented on the correct physical port and Virtual Path Identifier/Virtual Channel Identifier (VPI/VCI) value is transported across the network to the PVC termination point, in this case the OLO interconnection point. The ADSL access and backhaul networks in this case provide an alternative to leased line connections into traditional layer 2 services.

7.3 IPStream

IPStream is carried through the MSIP to the BT IP core network using an ATM PVC. A Point-to-Point Protocol (PPP) session originates from either the CPE ADSL device, or the PC (where this is connected via a USB connection to an ADSL modem), and is transported to a BAS. The BAS terminates the ATM PVC, but also invokes a PPP authentication process based upon the domain part of the username supplied by the ADSL site. The BAS is in this case a RADIUS client to the BT Platform Radius server, which contains profile information for this connection. By examining the domain part of the PPP authentication, the BAS establishes a compelled L2TP tunnel to the correct far end L2TP Network Server. For example, ANOther@anyISP.net would invoke the L2TP tunnel profile for anyISP.net, provided this profile is stored on the Platform RADIUS server.

The main aim of this RADIUS interrogation is to invoke the correct transport tunnel and other parameters, rather than to authenticate the ADSL endpoint. However information concerning the customer physical port is also held in the platform RADIUS, and can be used to ensure that only allowed service selections are made from a specific access point into the ADSL network.

This compelled L2TP tunnel runs across the Colossus core network; depending upon the wholesale service purchased, two different interconnect architectures are available, branded 'BT Central' and 'L2TP Pass Through' by BT.

In the BT Central architecture, the Colossus L2TP tunnel is terminated within the BT network on a 'Home Gateway'. This device includes L2TP Network Server (LNS) functionality, and so must be able to act as an authentication client for the downstream service provider or corporate network. To achieve this, the Home Gateway terminates the PPP session originating from the ADSL site, and handles user authentication and IP address configuration for the ADSL client. Since BT will not normally have direct access to the downstream authentication server in the OLO or corporate network, BT use a proxy RADIUS server to pass authentication information between the Home Gateway and the downstream RADIUS server in the OLO or corporate network.

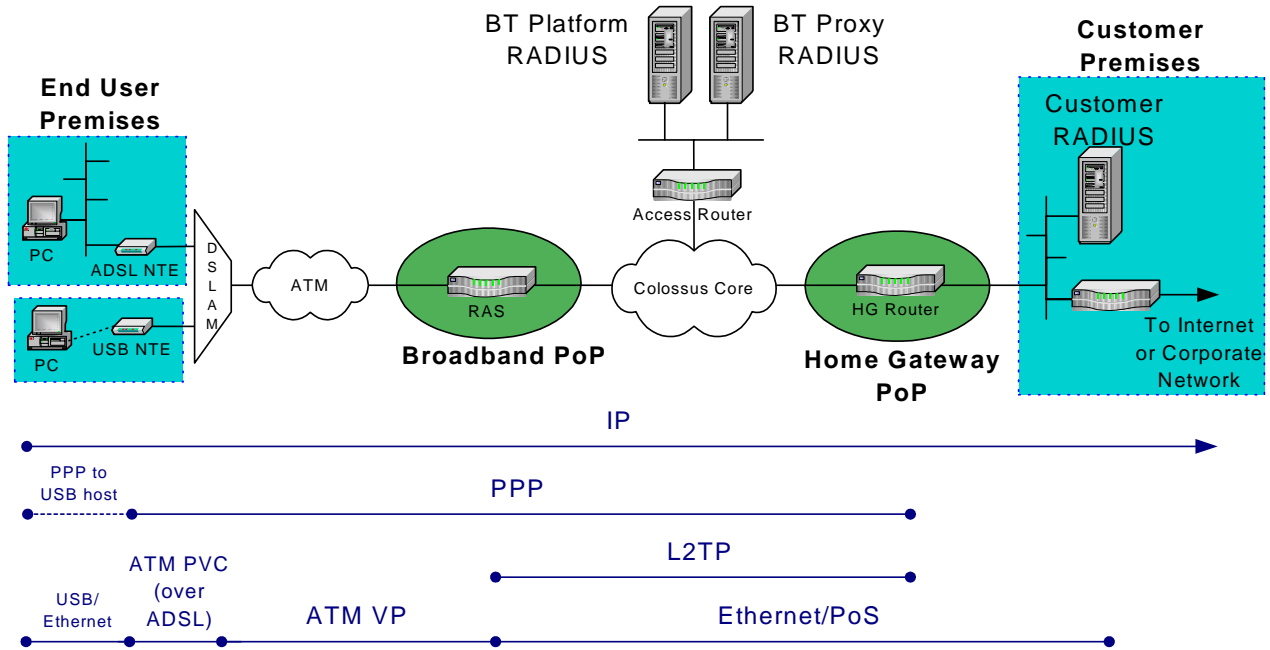


Figure A.3: Protocol architecture of IPStream with BT Central interconnect

In the L2TP 'Pass Through' architecture, BT aggregate the L2TP Colossus tunnels for a particular downstream customer into a smaller set of tunnels on an L2TP Tunnel switch at the egress from the Colossus network. The new aggregate L2TP tunnel is then passed across an ATM interconnect to the customer network. In this architecture, the PPP session from the ADSL site is terminated within the OLO network, and the normal PPP mechanisms for user authentication, IP address allocation, etc. can be applied in the OLO network to control access to whatever services are being provided. Therefore the BT proxy RADIUS is not used.

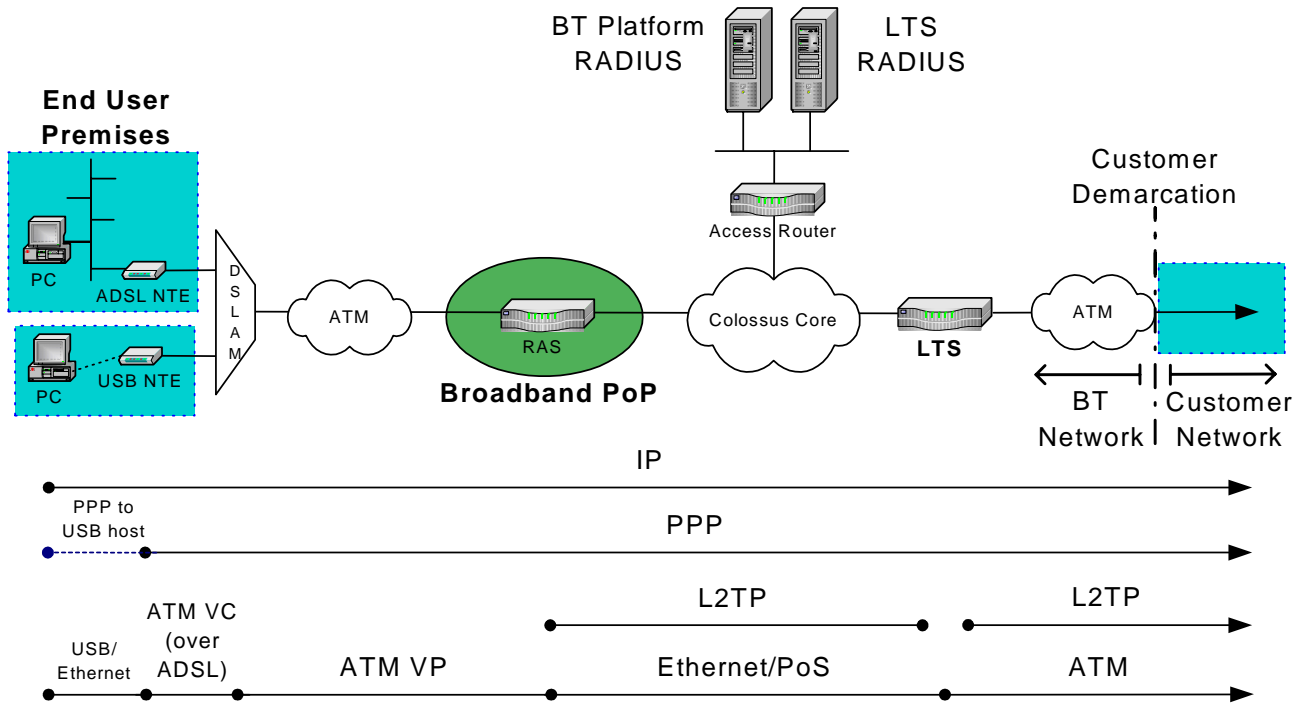


Figure A.3: Protocol architecture of IPStream with L2TP 'Pass Through' interconnect

7.4 Downstream Services

OLOs offer various downstream services based upon the BT ADSL wholesale solutions. Access to traditional Layer 2 VPNs is typically offered using the DataStream service. Access to downstream ISPs is typically offered across the IPStream service. ADSL access directly to corporate sites is offered using IPStream or DataStream. In evaluating the suitability of a solution for CNI use, the end-to-end solution, rather than simply the ADSL and backhaul components, must be considered.

7.5 ADSL Layer 2 services compared to traditional leased-line access to Layer 2 services

ADSL Layer 2 services such as BT DataStream provide a single PVC connection at Layer 2 between an ADSL CPE and the OLO interconnect point or end-customer site. The use of ADSL rather than a traditional leased line for access to the Layer 2 service mainly affects the physical Layer protocols in the access network. Provided good practice is applied to the design, implementation and operation of the service, this is considered equivalent to leased line access to a Layer 2 service.

7.6 xDSL Layer 2 Circuit Emulation Service (CES) compared to traditional leased line services

Where an ATM CES is offered across an ADSL or SDSL access network, the ATM backhaul network emulates a physical Layer leased line, either to an OLO connection point, or directly to the customer premises. These services are being trialled at present, and will be offered as a replacement or substitute for traditional leased lines in the short to medium term. Provided good practice is applied to the design, implementation and operation of the service, this is considered equivalent to a physical Layer leased line.

7.7 ADSL Layer 3 services compared to dial-up services

No simple equivalence between an IPStream-based service and a direct dial-up service exists when considered from an end-to-end perspective. However provided good practice is applied to the design, implementation and operation of the service, in particular concerning service selection, authentication and by layering end-to-end security services above the basic service (see section 4), then an end-to-end service based on IPStream (with appropriate layered cryptographic security) may be seen to be roughly equivalent to an Internet-based VPN.