INTERNET DRAFT Cleve Mickles (Co-Author)
Document: draft-mickles-v6ops-isp-cases-05.txt AOL Time Warner
Expires: Sept 2003 March 2003

Transition Scenarios for ISP Networks

Status of this Memo

Abstract

This document describes the different types of Internet Service Provider (ISP) networks in existence today. It will provide design and operational considerations in delivering network services to customers for seven specific areas in an effort to better identify specific issues which may arise during a transition to IPv6.

Table of Contents

1. Introduction

This document will describe the basic design of ISP networks today. It will be used to provide direction on what must be considered to transition IPv4 networks to IPv6. The main purpose of this document is to identify, and document the issues that must be considered before transitioning a network to IPv6. This document is not meant to determine exactly how the transition will occur for the various ISP networks. This document is not meant to describe how to build an IPv6 network from scratch. This document will not describe what is or is not a "Tier 1" or "Tier 2"..."Tier N" ISP. The document focuses on IP capable network devices and may reference non-IP related devices for clarification purposes only.

2. Scope of the document

The scope of this document is to cover the major topics ISPs must consider in building and running their IP networks. The following sections include descriptions and design considerations for Core backbone networks, Broadband DSL
networks, Broadband HFC Cable networks, Narrowband Dialup networks, Public Wireless LAN Networks, Broadband Ethernet and Public Exchange Point networks. The document will also identify Security and Network Management concerns which in some cases will be common to all as well some areas that may be unique to the particular service. In some cases a single ISP may provide services in more than one of the areas mentioned below.

Although the Optical core is important in today's networks, that layer is generally transparent to the IP layer except in a few special cases where ISPs have allowed the IP core to be aware of the optical layer underneath. Hence, this draft does not include further optical considerations.
Each scenario will discuss issues related to network topology, network hardware, routing, policing, security, network management, configuration and host gear.

3. Core/Backbone Networks

This section describes the general topologies of and characteristics of today's CORE networks. Although there are numerous large scale networks out there today, most employ the same basic set of principles when designing and building their networks.

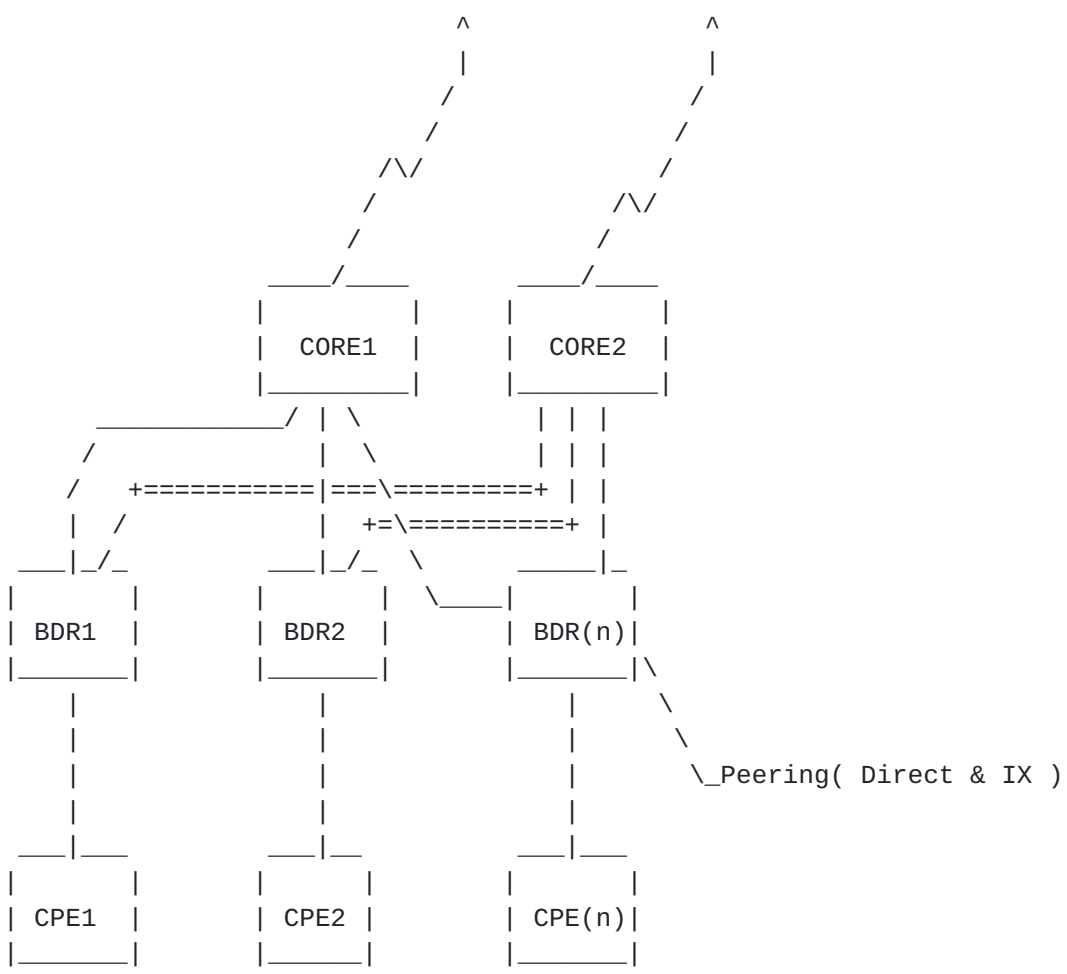


Figure 3.1

3.1 Topology

In terms of physical equipment, today's backbone networks consist mainly of high-speed routers that are configured in a basic core and edge configuration. In most configurations, for redundancy, there are two or more core routers as well as two or more border routers. The border routers provide any local connectivity and peering. Generally filtering, routing policy and policing type functions are done on the border routers. The core routers provide aggregation of border router traffic as well as

aggregation of long haul circuits to remote sites. The physical topology is depicted in Figure 3.1.

The logical topology includes the core routers being IBGP peers with every other POP in the mesh. The local border routers are route reflector clients of the core.

3.2. Hardware

The hardware deployed in the CORE Backbone is similar across ISPs and generally consists of high-speed routers. The requirement for switches in the CORE network is for infrastructure type hosting gear. In some cases CPE equipment is provided by the CORE ISP.

3.3. Routing

An assumption is that all routers in the core will have some IPv4 reachability. As the network grows additional routers may be added which only have IPv6 reachability but most routers which support IPv6 networking will be dual stack.

In the routing area ISPs must consider how IPv6 traffic will be exchanged over the link layer of the network. There are two cases which are available. Either all routers within the network will be IPv6 capable or a disjoint subset of routers will have IPv6 capabilties. This decision will determine whether IPv6 addressing is configured over each IPv4 point to point link or the more likely scenario is configuring IPv6 on some point to point links and tunneling IPv6 over IPv4 to reach other network devices.

3.3.1 IGP

Internally Core ISPs generally use OSPF or ISIS as an IGP. Loopback interfaces and point-to-point links are what make up routes within the IGP.

Once the IPv6 link layer topology has be determined the IPv6 IGP choice must be made. The choices in the Core network include basically OSPF or ISIS for IPv6 routing. For networks which have deployed one or the other for IPv4 traffic, the ISP must consider the ramifications of the choice.

Case 1: Existing OSPF IPv4 network

If the ISP chooses to build IPv6 capabilities using OSPFv3, then considerations of existing hardware and memory constraints must be made since OSPFv3 places additional load on network gear. This IGP will operate in separate memory space and will need to be configured separately from any existing OSPFv1 implementation.

If the ISP chooses to build IPv6 capabilities using ISIS, then considerations of existing hardware and memory must constraints must be made as adding ISIS to an existing OSPFv1 implementation. The amount of hardware resources are not as taxing. As with the OSPF scenario, ISIS would be configured separately from the existing OSPFv1 implementation.

Case 2: Existing ISIS IPv4 network

If the ISP chooses to build IPv6 capabilities using OSPFv3, then considerations of existing hardware and memory constraints must be made since OSPFv3 places additional load on network gear. This IGP will operate in separate memory space and will need to be configured separately from any existing ISIS implementation.

If the ISP chooses to build IPv6 capabilities using ISIS, then the amount of hardware resources are not as taxing since IPv6 is integrated within ISIS. The protocol does not need to be configured separately.

3.3.2 EGP

Generally BGP4 is the Edge gateway protocol of choice. The EGP routing table consists of networks, which are received via customer advertisements, statically configured for customers who are not running a dynamic routing protocol or networks that are nailed up as part of the ISP infrastructure.

A decision must be made on whether the exchange IPv6 routes via BGP4+ or to use static addressing with each neighbor.

3.3.3 IRR & Routing Policy

Routing policy on the core includes multiple peer-groups setup to represent a collection of customers, external peers or internal peers. In the case of customer connections, there are peer groups that are configured to send FULL_ROUTES, CUSTOMER-ROUTES or DEFAULT-ROUTES to a particular set of customers. To perform this function, the peer groups reference ROUTE-MAPs. External peers generally fit into the CUSTOMER_ROUTES peer group. In the case of internal peers an INTERNAL peer group is used to identify internal routers that carry backbone circuits and an RRCLIENT peer-group is created to group border routers with a common set of characteristics.

Assuming most Core providers are using BGP4 to exchange IPv4 routes the providers will have multiple routing policies and various peer groups setup for IPv4 neighbors. A sample of these various policies are noted above. A choice must be made as to whether to create parallel sets of routing policy for IPv6 neighbors whether they are INTERNAL or EXTERNAL to the network. A decision on where/how to register IPv6 routing policy in the IRR must be done as well.

3.3.4 Multicast

PIM-SM is the generally accepted solution for deploying multicast.

For IPv6, this is a hard problem.

3.3.5 Addressing

Addressing in the Core of the network has two components. The infrastructure routers have requirements for loopback and point-to-point addresses. These addresses are routed within the IGP. Customer routes are pinned up on core routers.

In the area of IPv6 addressing, the core providers should determine whether create additional IPv6 loopback interfaces as well as decide whether to add IPv6 addresses on all point to point links along side IPv4 addresses. As with IPv4 aggregate routes, the core provider must determine whether IPv6 aggregate routes should be "pinned up" or advertised from the edge network.

3.3.6 NAT

NAT may be deployed in the Core provider networks only in special cases.

In terms of IPv6 routing in the core, IPv4 NATs should be avoided when trying to exchange IPv6 traffic.

3.3.7 Aggregation

Aggregation of routes in the Core networks should be done. Networks that are used for loopbacks and interfaces should be aggregated prior to being advertised externally. Generally aggregated "pin up" routes are placed on routers that carry backbone trunks.

For IPv6, ISPs must choose whether they will aggregate loopbacks and interfaces as is done in IPv4.

3.4. Traffic Engineering

Core providers have few choices in terms of traffic engineering. One method is MPLS. To use MPLS, a provider only needs a traffic matrix of next-hop data from within their network. Once a provider knows how much traffic is sent between all routers in the network, MPLS tunnels can be built to steer traffic over the optimum path to deliver all traffic. This scheme is analogous to the use of ATM PVCs over OC-12 circuits in prior years. Most networks employ some type of traffic engineering mechanism to steer traffic around potentially congestive areas. Beyond the standard methods of TE, some ISPs attempt to adjust metrics or cost on p2p links to perform TE. An additional method involves using varying BGP routing announcements to increase or decrease traffic on a particular link. Finally, there are also networks that employ an over provisioning model to limit packet loss. This involves adding capacity above and beyond what is needed.

Core ISPs must consider whether to deploy IPv6 traffic engineering mechanisms to control the flow of IPv6 traffic through the network. IPv6 has inherent advantages to perform native traffic engineering or the provider may use existing IPv4 "tweaks" to control IPv6 traffic flow.

3.5. Security

In the Core provider's network, security has a specific scope. Securing a network is typically done on the border or edge router. Generally an attempt is made to filter BOGON(RFC 1918) routes, traffic sourced from unallocated address space or sourced from address ranges that are internal to the local ISP. In some cases, hosts that support the infrastructure network equipment generally have filters in place to protect those hosts from outside attacks.

In many Core networks, there is IPv4 filtering in place for many reasons. The ISP must determine whether adding IPv6 filtering policy to the current set of policy will add the protection needed and allow the network to remain stable.

3.5.1 Intrusion Detection

Intrusion detection mechanisms and systems are used to protect infrastructure and host gear. Generally these intrusion detection systems are placed at various points within the network to search for vulnerabilities within the infrastructure as well as monitor activity that may be considered suspicious.

For IPv6 intrusion detection may be more difficult to perform due to the large subnet size generally deployed in IPv6 networks. The average subnet is a /64 network which makes random scans by attackers less effective. There are cases where known server systems which may be published in DNS may be targeted. The ISP must choose whether to deploy IPv6 intrusion detection mechanisms prior to implementing IPv6.

3.5.2 Ingress Filtering

Ingress filtering on Core networks comes in multiple flavors. For providers that do filter, the first level is EGP filtering. When a peering session is setup, ISPs require a peer to register their routes in an IRR and that data is used to create an EGP filter on the peering session to only accept registered advertised routes. A step beyond this includes Reverse Path Forwarding (RPF) checks to verify that traffic sourced from the customer link is within the advertised range. An alternative to the automated RPF checks is the brute force static packet filters which can be used to control traffic sourced from a particular customer link.

For IPv6, Core providers must determine whether to implement similar ingress filtering mechanisms which are currently deployed in IPv4 networks.

3.6. Network Management

Devices within the network must be monitored. This is done over in-band connections to the network devices. Generally there are filters on the routers to allow SNMP queries from the query server.

3.6.1 Out of band

Out of band networks allow access to consoles of the network gear. In some cases this access is done in-band. There are also cases where separate networks are built to allow access.

The Core ISP must determine whether to convert it's out of band network to IPv6 or not.

3.6.2 Configuration Tools

Many ISPs have monitoring tools that query the network gear to gather data. These scripts may be written in perl or expect and will access the device via the CLI over the in-band ipv4 connection.

The ISP must determine whether support servers will have the ability to contact network gear over native IPv6 connections or not.

3.6.3 SNMP

Statistical monitoring of network gear is done via SNMP queries. These queries are done via the in-band connection.

The ISP must decide whether Network Management devices will contact infrastructure over native IPv6 or IPv4 connections.

3.7. Hosting Gear

In terms of host gear, the Core networks maintain hosts for supporting and managing the network, but not necessarily the end user. The standard set of hosts include DNS servers, mail gateways, authentication(RADIUS or TACACS), and network management servers. The servers are distributed to strategic locations for diversity purposes. Servers included in this model include DNS and TACACS servers that directly support the operator's network. Reachability to the servers is over an IPv4 routed connection. Caching infrastructure is deployed in CORE provider networks in a very limited fashion to assist in reducing the traffic pulled from external sources.

For IPv6, providers must decide whether to deploy parallel host infrastructure for IPv6. Other considerations include whether all existing host infrastructure should have IPv6 reachability.

4. Broadband HFC/Coax Networks

This section describes the infrastructure that exists in today's HFC cable networks that support cable modem services to the home. Since many cable providers are regional they generally have used the backbone ISP networks for transit IP services beyond their region.

4.1 Terminology

HFC network: Hybrid Fiber Coaxial network
CM: Cable Modem
CMTS: Cable Modem Termination System
CPE: Customer Premises Equipment
DOCSIS: Data Over Cable Service Interface Specification -- the standards defining how data should be carried on HFC networks

4.2 Topology

4.2.1 Physical

HFC networks are a mix of fiber optic and coaxial cables originally designed for the delivery of cable television. A single infrastructure can support video distribution, data networking and telephony. Video and data signals are typically sourced from different systems and frequency division multiplexed over the HFC network. Historically HFC networks were uni-directional and required some kind of telco-return path to support bi-directional data. Today much of the cable infrastructure has been upgraded to support return paths over the HFC network.
A CMTS can serve quite a large geographic area: 10s of miles radius is not uncommon and DOCSIS specifies a 100 mile diameter upper limit.
In a DOCSIS system, down-stream and up-stream channels are distinct and occupy different frequency bands. A CMTS may terminate multiple up and downstream channels and a CM must tune in to an up-stream and down-stream channels before communicating. All packets on the HFC network are forwarded via the CMTS. Cable modems may forward packets between network segments attached to CPE. Hundreds of hosts on a cable network may be part of the same broadcast domain.

4.2.2 Logical

DOCSIS systems are designed to transport IP traffic. The following two paragraphs are present in all current DOCSIS specifications.

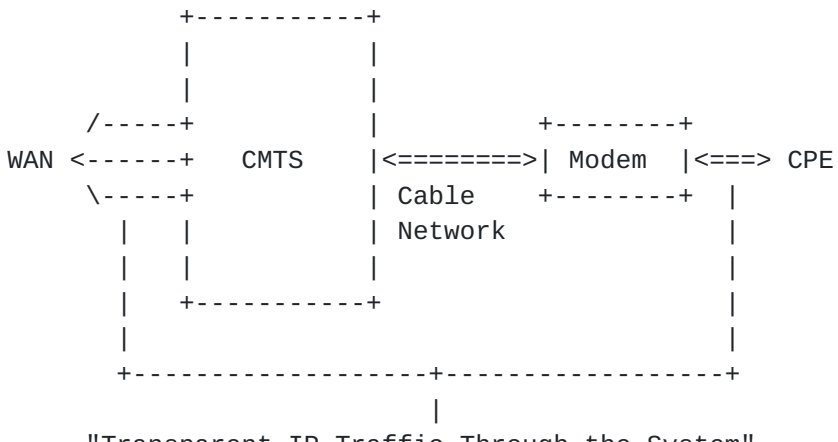
Section 1.3.1 [DOCSIS-1.1]:

"The intended service will allow transparent bi-directional transfer of Internet Protocol (IP) traffic, between the cable system headed and customer locations, over an all-coaxial or hybrid-fiber/coax(HFC) cable network."

Section 3.2.2.1 [DOCSIS-1.1]:

"Forwarding of IP traffic MUST be supported. Other network layer protocols MAY be supported. The ability to restrict the network layer to a single protocol such as IP MUST be supported."

In the context of the [DOCSIS-1.0], [DOCSIS-1.1] and [DOCSIS-2.0] specifications "Internet Protocol (IP) traffic" means IPv4 traffic. The following diagram(Figure 5.2.2) has been reproduced from the DOCSIS RFI specification [DOCSIS-1.1] and slightly simplified:



"Transparent IP Traffic Through the System"

Figure 4.2.2

Note that between the WAN and the CPE, both forwarding at Layer-2 (bridging) and at Layer-3 (routing) will meet the goal of transparent transport of IP traffic.

4.3. Hardware

4.3.1 Cable Modems

Cable modems operate as transparent L2 bridges forwarding datagrams from the HFC network to the CPE network.

Cable modems use a combination of policy settings and IGMPv2[RFC2236] to control multicast forwarding (see Section 3.3.1 [DOCSIS-1.1]).
Forwarding of IPv6 multicast datagrams may not occur properly as CMs are required to forward multicast datagrams only when CPE equipment has joined that group. This is potentially a show-stopper if native IPv6 Neighbor Discovery[RFC2461] is being used through a CM.

4.3.2 CMTS Layer-2 Bridge

A DOCSIS compliant CMTS may be implemented as a Layer-2 transparent bridge. Forwarding of IPv4 packets by the transparent bridge is mandatory and forwarding of other protocols may be supported. It is likely that implementers using this approach will support forwarding of arbitrary protocols using 802.1d hence forwarding of native IPv6 datagrams should just work. IPv6 is then deployed on the ISP router infrastructure natively or using an automatic tunneling scheme like 6to4[RFC3056]. As with the CM, a bridged CMTS that selectively forwards multicast datagrams on the basis of IGMPv2 will potentially break IPv6 ND. This behavior is recommended but not mandated for a Layer-2 CMTS. Communication between CPE behind different cable modems is always forwarded by the CMTS. IPv6 communication between the different sites relies on multicast IPv6 Neighbor Discovery [RFC2461] frames being forwarded correctly by the CM and the CMTS.

4.3.3 CMTS IP Router

A DOCSIS compliant CMTS may be implemented as a Layer-3 IPv4 router. In this case IPv6 packets passing from the WAN network to CPE must be encapsulated in IPv4. Forwarding between channels on the HFC network (i.e. within a CMTS) may still take place at L2 hence the comments in Section 3.2 may also apply.
A CMTS may also be an IPv6 router and thus support IPv6 natively.

4.3.4 IPv4 NAT CPE routers

A fairly common CPE device in HFC networks is the IPv4 NAT/DHCP router. It is usually connected between the cable modem and all other CPE equipment allows multiple devices to share a single IPv4 address and cable modem connection with a minimum of configuration overhead. The NAT/DHCP router is a directional IPv4-only device in the communication path between the CMTS and the CPE. Unfortunately the IPv4 NAT router prevents (or at least seriously complicates) the deployment of IPv6 in a number of ways:

o As an IPv4-only device it will block native IPv6 frames forwarded through the cable modem.

- o The use of private addresses on the CPE network means that schemes relying on global IPv4 addresses (e.g. 6to4[RFC3056]) cannot be used.
- o Many NAT/DHCP routers only support forwarding of a limited number of IPv4 protocols (e.g. TCP, UDP, ICMP) and will drop IPv4 encapsulated IPv6 with an "unknown" protocol number (e.g. 6to4 packets).

In an ideal world every IPv4 NAT router would be upgraded to additionally become a native IPv6 router using 6to4 automatic tunneling.
In general 6to4 residential gateway devices must be made as self-configuring as existing IPv4 NAT routers.

4.4 Routing

There are no known HFC-specific routing issues.
Cable networks are typically access networks. If the CMTS is a native IPv6 router then it will likely need to participate in ISPs the IGP of choice. If the CMTS is a bridge, the infrastructure router(s) that it connects to will need to speak an IGP. If 6to4[RFC3056] is used, it is recommended that the ISP sink (and forward) traffic to the anycast 6to4 relay router address [RFC3068].

4.5 Policing

Cable networks are large shared subnets. Filtering is extensively used in this environment to ensure stability of the network and to protect subscribers. For example, filters are used to prevent CPE DHCP server responses from escaping from the CPE network. As a security measure, filters are very often deployed to prevent file sharing protocols leaking between different CPE sites.
IPv6 opens up a new communication channel. Existing IPv4 filter software will not block IPv6 communication. If IPv6 is tunneled over an IPv4 infrastructure filters may need to examine the contents of encapsulated packets.

4.6 Security

CPE NAT boxes are rectifying routers. This can be viewed as an implementation of an "outgoing only" security policy. IPv6 devices need to be able to support a similar kind of policy.

4.7 Network Management

DOCSIS cable modems use an out of band, privately addressed IPv4 network for configuration and network management functions.
DOCSIS cable modems and CMTS are IPv4 hosts on the out of band management network. At present there is no compelling need to update this network to support IPv6.
DOCSIS cable modems use:

- SNMP [RFC1157] for network management.
- TFTP [RFC1350] for software and configuration parameter download
- DHCP [RFC2131] for acquiring IPv4 address, etc allowing communication on the management network.
- ToD [RFC0868] for initial time synchronization.

Various MIBs for RF and CPE filter configuration.. DOCSIS OSSI docs override the IETF MIB specifications. Any IPv6 issues in there?

4.8 Host Gear

Dual stack DNS server is necessary if you want to support IPv6-only CPE equipment.
DDNS is pretty much mandatory if you want to give CPE devices DNS names. This is because only the IPv6 host knows what its full IPv6 address is (esp when privacy addresses are used).
Transition functionality.. which? where?
v4/v6 translation between devices in the home is done where? If RFC1918 addresses are in use (perhaps behind the NAT), then there isn't much choice but to do it inside the CPE box.
Transparent proxy caches aren't going to cache IPv6 web traffic.

5. Broadband DSL Networks

This section describes the infrastructure that exists in todays High Speed DSL Networks.

5.1 DSL physical architecture

Digital Subscriber Line (DSL) technology is a modem technology that allows subscribers to perform access from the home or office to broadband network services by using existing twisted-pair copper wire telephone lines.
The term xDSL is the generic name that has been given to the family of digital subscriber line technologies, including ADSL, SDSL, HDSL, VDSL, and IDSL.
The POTS (Plain Old Telephone Service) takes only the frequency range 0-3000 Hz but there is considerably more bandwidth on these copper lines; DSL gets more from them by using sophisticated digital coding and splitting the line (reserving the higher frequencies for data, the lower for voice and fax) to achieve high-speed data transmission over the local loop from the customer site to a service provider's switching center. But the bandwidth a subscriber can receive depends on the quality of the line and on the distance to the service provider's center. Distance can be increased, but then speed is reduced. For instance, it is possible to use ADSL up to 18,000 feet, but the maximum downstream speed is then reduced to 1544 kbps. Several models are used to deploy IP over DSL services, but all use the same components:

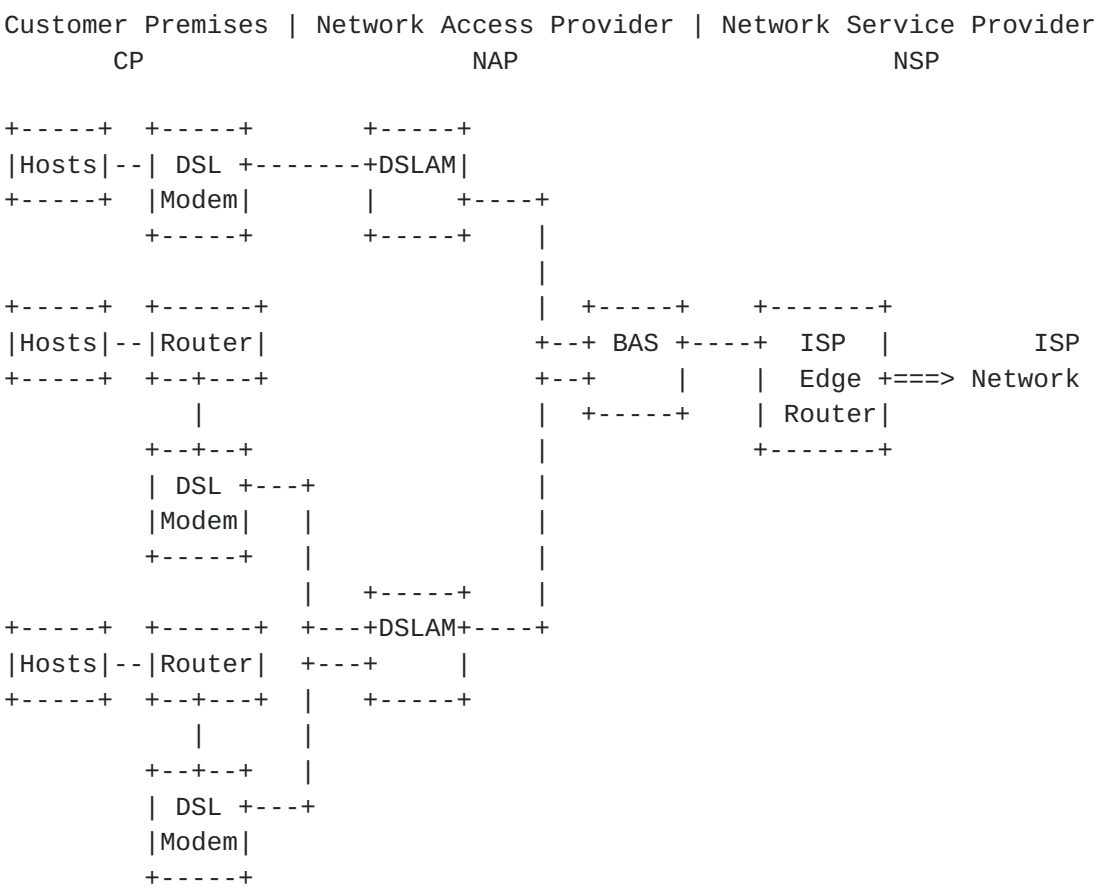


Figure 5.1

The hosts are connected to the DSL network either directly through a modem, either through a router and a modem. The modems may be included in the hosts or in the routers. When it is not the case, the DSL modems may be accessed through ATM, Ethernet or USB. It must be noted that when a router is used in customer premises, it often has only very limited resources in terms of memory or processing power.

IP packets are then transported on twisted-pair telephone lines to the NAP's DSLAM (DSL Access Multiplexer), thanks to DSL technology. The DSLAM terminates and multiplexes several DSL accesses to the NAP's backbone. It forwards data to the BAS (Broadband Access Server = DSLAM aggregator), which is in charge of directing them to the POP (Point Of Presence = the ISP Edge Router) of the NSP that the client has subscribed to. Note that NAP and NSP can be the same organization. The technology used in the NAP network is usually ATM, but other types of layer 2 technologies may be used.

This model enables the local operator to make its local copper available to other companies. Operators are then able to offer DSL technology for broadband Internet access.

As the access network puts service users in communication with their NSPs, security and access control are required.

5.2 Logical architectures used today for IPv4 access

Data transport between the CPE and the service provider's point of presence (POP) generally relies on an ATM based infrastructure. Two types of use of this infrastructure are common:
* ATM point-to-point model: one PVC connects each subscriber to its NSP. From the Broadband Access Server (BAS), there are exactly as many PVCs across the NAP network as the number of subscribers (i.e. one PVC per subscriber). This model is detailed in section 5.2.1.
* Aggregation model: the BAS aggregates multiple subscriber PVCs into trunk PVCs to reduce the number of PVC connections across the NAP core network (one PVC provisioned for many subscribers to the same destination NSP, or if the NSP offers multiple service levels, more than one PVC could be established across the core). There are two usual ways to aggregate connections:
- PPP Terminated Aggregation (PTA): PPP sessions are opened between each subscriber and the BAS. The BAS terminates PPP sessions and transfers subscriber's traffic up to the POP. This model is detailed in section 5.2.2.
- L2TP Access Aggregation (LAA): PPP sessions are opened between each subscriber and the POP. The BAS dispatches PPP sessions up to the POP, by encapsulating them into L2TP tunnels. This model is detailed in section 5.2.3.

5.2.1 ATM POINT-TO-POINT MODEL

This model is adapted to networks with few subscribers and static configuration. It is simple to deploy but it cannot be used in large networks.
In this model, each subscriber is connected to its NSP via one PVC. The user network IP packets are transmitted frames from the CPE to the DSL modem or router. There, RFC 2684 bridging occurs: The LAN frames are forwarded into an ATM PVC (segmenting them into ATM cells through AAL5).

The following figure describes the protocol architecture of this model.

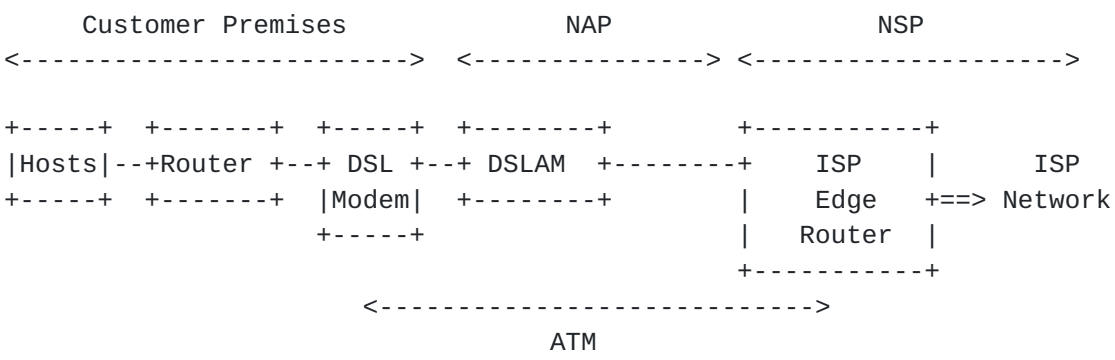


Figure 5.2.1

Since the CPE is in bridging mode, this model is layer 3-independent and the NAP is free of addressing and routing concerns. The NSP edge router sees all subscribers as attached to the same Ethernet link. Very complex controls and restrictions must thus be performed to avoid spoofing and broadcast storms. Last, subscribers do not have access to multiple ISPs over a single DSL line.

5.2.2 PPP TERMINATED AGGREGATION (PTA) MODEL

The PTA architecture relies on PPP-based technologies (PPPoA and PPPoE), terminated at the BAS. The BAS has at least one PVC opened to each NSP, but several PVCs are sometimes used when the NSP offers differentiated services (QoS...).
In this architecture, the aggregator BAS provides PPP session termination and the subscriber data is then forwarded to the NSP's edge router using IP over ATM.

Since the PPP session is terminated at the BAS, the BAS must perform per session authentication, authorization and accounting on behalf of the NSP, and perform layer 3 routing. The PTA architecture has several advantages. First, it reduces the number of PVCs used in the NAP core network. Second, it offers the subscribers the capability to choose between several NSPs. However, it is not as flexible as the LAA model from this point of view: it requires strong coordination between the NSP and the NAP. This model is often used when the NSP is also the NAP.

5.2.2.1 Connection using PPPoA

The following figure describes the protocol architecture of this model.

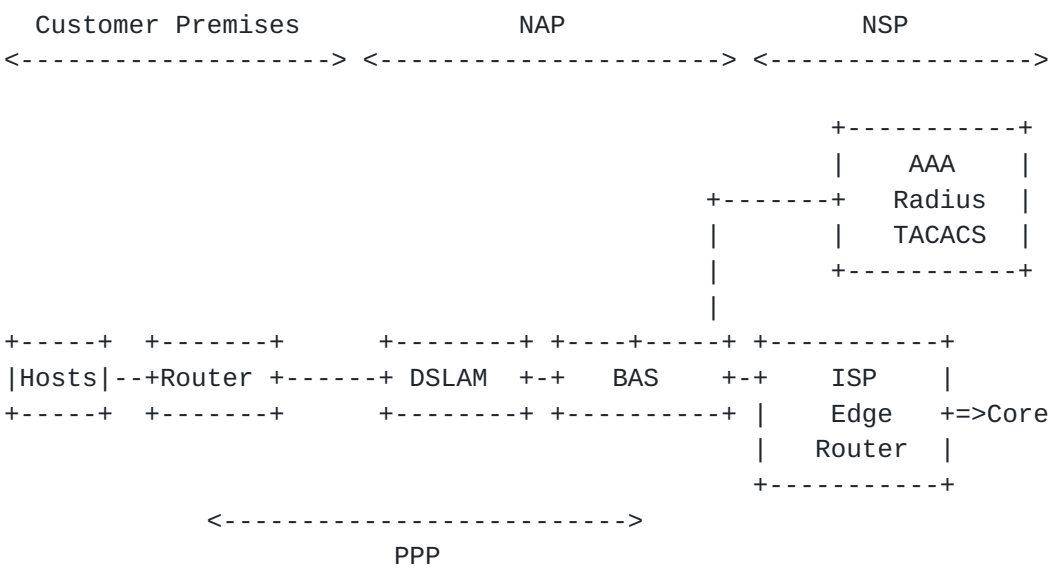


Figure 5.2.2.1

The PPP sessions initiated by the CPEs are terminated at the aggregation device (BAS), which authenticates users either by using a local database or by sending a request to a remote server located at the NSP (a RADIUS server for instance). When RADIUS is used, a user can be authenticated based on a username or based on the VPI/VCI used. There is only one PPP session per ATM PVC.

Upon successful authentication, the customer premises equipment may then be configured dynamically. Of course, static configuration is also possible. When dynamic configuration is used, the BAS obtains the address of a DNS server and an IPv4 address or prefix for the customer, usually through a DHCP server or a RADIUS server. The BAS then sends this information to the CPE via IPCP, and establishes a new route between the CPE and the BAS.

5.2.2.2 Connection using PPPoE

The following figure describes the protocol architecture of this model.

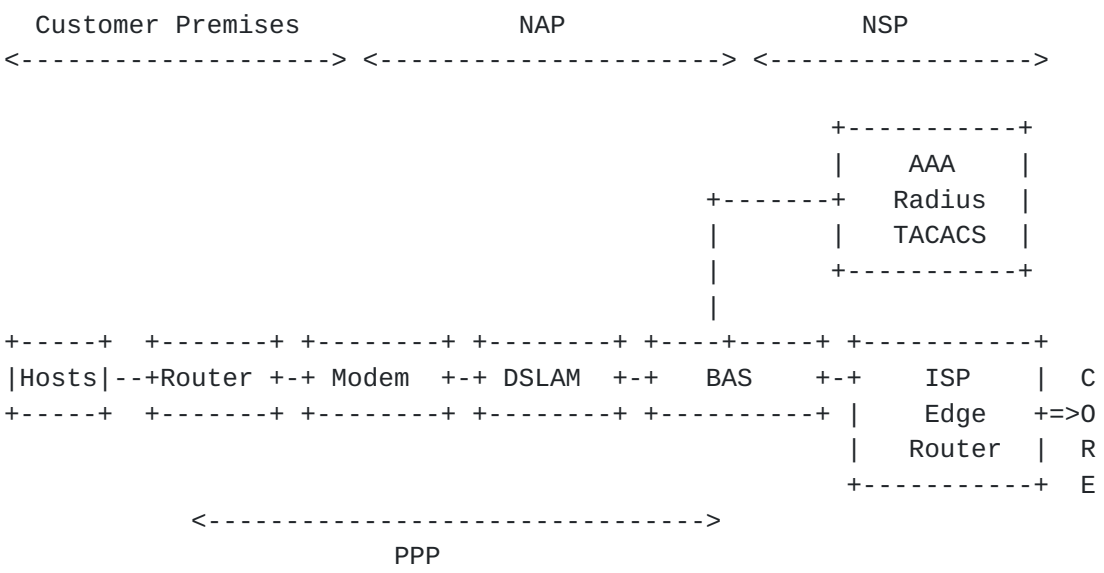


Figure 5.2.2.2

The PPPoE-based PTA model is more flexible than the PPPoA based one: several PPP sessions may be opened with the BAS at the same time, over as many PPPoE sessions. This allows subscriber to access several services at the same time, on the same VC.
The authentication process is the same as the PPPoA one except that VPI/VCI-based authentication cannot be used.
It must be noted that the extra PPPoE encapsulation reduces the IP MTU and MRU, because two PPP and PPPoE headers (2+6 bytes) are inserted between the IP packet and the Ethernet header. This also results in a decrease of the MSS of TCP that applications should use.

5.2.3 L2TP ACCESS AGGREGATION (LAA) MODEL

While PTA model terminates PPP sessions at the aggregation device and then forwards IP traffic to its destination, LAA model allows forwarding PPP sessions from subscribers to the NSP's point of presence, via a L2TP tunnel. When a CPE initiates a session with its NSP, the BAS intercepts the PPP connection request. It reads the PPP identities of the subscriber and of the NSP, and sends a request to the NSP's RADIUS server, asking for the address of the device to which the PPP connection should be forwarded.
If not opened yet, a L2TP tunnel is established between the BAS and the NSP's server. The PPP connection is then encapsulated and forwarded into this tunnel. User authentication and dynamic configuration are performed by the NSP itself.

5.2.3.1 Connection via PPPoA

The following figure describes the protocol architecture of this model.

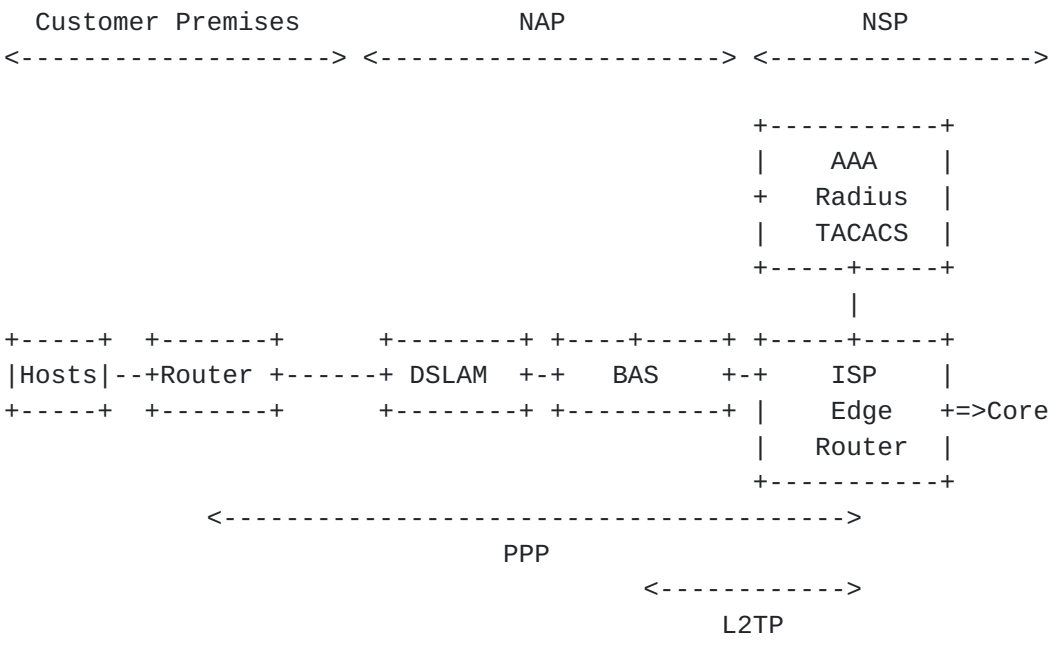


Figure 5.2.3.1

5.2.3.2 Connection via PPPoE

The following figure describes the protocol architecture of this model.

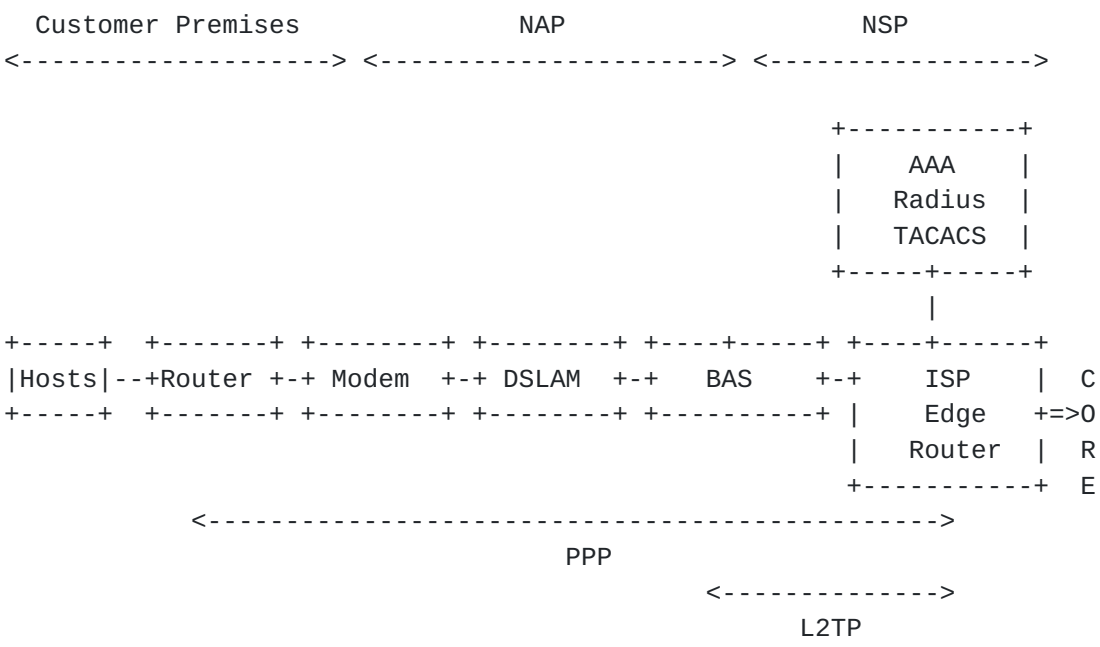


Figure 5.2.3.2

5.2.4 OPTIMAL MTU CONFIGURATION FOR DSL CONNECTIONS USING PPPOE

While PPPoA does not impact the default MTU on an LAN environment (1500 bytes), PPPoE induces a smaller MTU (1492 bytes, 1500 bytes minus 2 bytes for PPP header and 6 bytes for PPPoE header). This causes some problems, especially when ICMP error messages such as "Packet Too Big' are filtered by intermediate nodes.

5.3 ADDRESSING FOR TODAY'S IPv4 ACCESS

One of the benefits of DSL for the customer is the capability to enjoy a permanent connection to the Internet on the telephone line. This allows the customers to use peer-to-peer applications and to set up servers when they are given stable global IP addresses. However, some service providers do not supply static addresses by default, and a lot of customers are using dynamic addresses today. Customers are usually disconnected every day and are given a new address each time they reconnect. Most of the times, customers use private addressing on their LAN and the access routers then perform NAT for Internet access. Some small ISPs do not even provide global addresses to their customers. These ISPs then operate NATs on their backbones.

5.4 ROUTING

Customers of DSL services may run routing protocols on their LAN (usually RIP or OSPF), but these LANs are usually small and do not require the use of a routing protocol.
When a router is used in the customer premises, it is usually configured with a default route to the NSP's edge router. In case of multi-homing, the customer's router may use BGP.
The NAP may have to run an IGP (OSPF or IS-IS).
Usually, the NSP uses an IGP (OSPF or IS-IS) on its core network.

5.5 DNS

Very often, the domain name of the customer is managed by the NSP and the domain name server is also hosted by the NSP.
In fewer cases, the customer hosts the server on its own LAN.

5.6 Network management

Usually, NSPs manage the edge routers by SNMP. The management stations are located on the core network.
Very few service providers manage equipment located on customers LANs. The use of NAT on the customer edge router forbids this type of service.

6. Narrowband Dialup Networks

This section describes Narrowband dialup networks that the majority of internet users use today to get online. The scenarios will include solutions where the dial infrastructure is controlled by one entity as well as solutions where ISPs lease modems from a wholesale modem providers.
There are multiple types of dialup services from plain/no frills access to the Internet, to wholesale dialup networks that can purchased by an organization wanting to resell internet services, and then there are the full service dialup providers that provide a long list of features to the end user. Generally smaller dialup ISPs purchase a T1 or greater facility from a Local Exchange Carrier(LEC) to the facility where modem equipment is housed. The choice in terms of the number of T1s (or other) is made dependent on how many simultaneous users are supported in the ISP's business model. Depending on the coverage area multiple phone numbers may be provided for the end-user to dial and the LEC may choose to route all calls to a common termination point or provide the traffic across multiple T1 facilities. When an end-user dials an access number, the LEC routes the call to the modem server location and is generally mapped by the LEC into a T1 facility that terminates on the modem server. The modem server attempts to verify the user credentials by querying the authentication server via an IP interface on the modem server. The modem server is present on a LAN network segment along with any relevant hosts as well as the default gateway router. Some services that are common to all dialup providers include the ability to provide DNS service either primary or secondary and an authentication server. The wholesale dial provider builds out the dial network just as the small dialup provider does. Differences include the ability of the wholesale provider to hand off aggregated traffic to the organization purchasing wholesale access or to allow the aggregated traffic to reach the Internet at large without the purchasing organization needing major internet access facilities. Each case has different implications.

The infrastructure used in the foundation of these various offerings is somewhat similar although the deployments vary depending on the level of service offered. The basic dialup service provider model that includes modem access to the Internet can be built from a terminal server (generally a digital modem bank), a Layer 2 switch and routers. For global reachability the dialup provider must connect to a backbone provider. The basic design calls for the terminal server to be attached to a layer 2 switch that would in turn have connections to a router. For redundancy, a dialup

provider can spread multiple shelves of terminal servers across individual routers and manually shift traffic if a router becomes disabled. A more robust redundant solution would be to deploy pairs of routers and use some Router Redundancy Protocol functionality to maintain traffic in the event of a failure of one router.

6.1 Topology

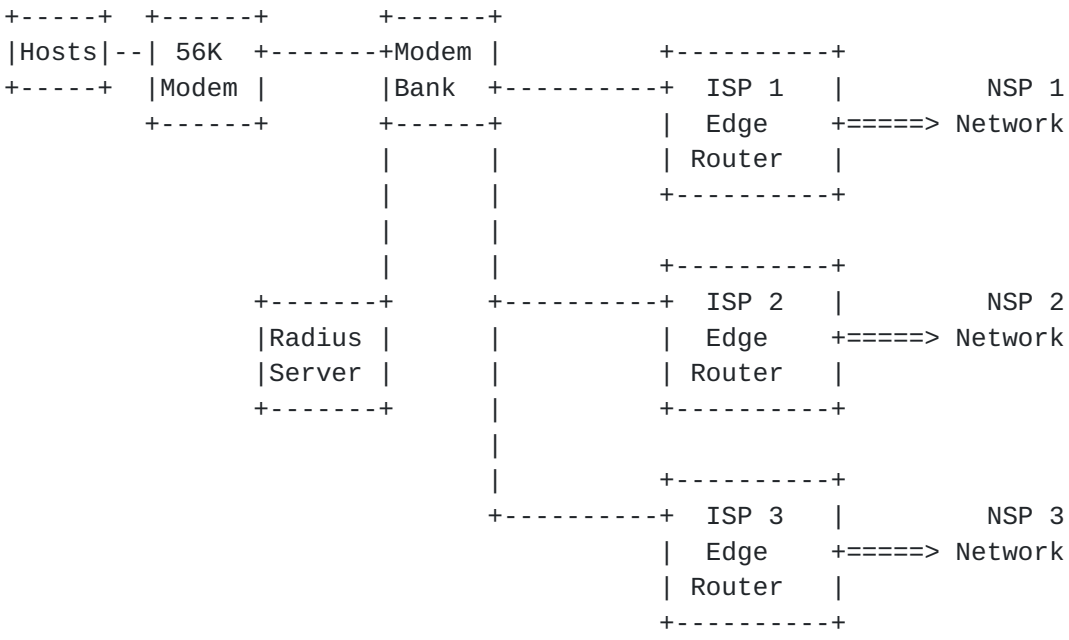


Figure 6.1

6.2. Hardware

The hardware involved in dialup service provider connections include the CPE device that is usually a 56K modem, the Terminal server/modem bank and an authentication server.

6.3. Routing

From the host device the user connects to the terminal server using Point-to-Point Protocol (PPP). Once the PPP connection is made the user credentials are sent to the Authentication server. The user is then assigned an IP address and then the connection is forwarded to the appropriate Internet Service Provider (ISP) and then on to a Network Service Provider (NSP). The NSP and ISP network can be external or internal to the dialup service provider.

In some cases Dial-up service providers will use Network Address Translation (NAT) to connect to external networks. NAT is only required if the address assigned by the authentication server is not a public address. Routing protocols such as an IGP or EGP will only come into play between the ISP and NSP networks. The address space required at a point of presence (POP) is determined by summing the number of modem ports available at a POP. IRR routing policy is generally registered by the ISP or NSP but in some cases the dialup provider may register policy.

For IPv6, the Dial-up provider must consider the location of IPv4 NAT devices since IPv6 traffic does not pass through NAT devices. This ISP must also consider how traffic will be exchanged with the NSP. The choice will be determined by whether the existing NSP router has IPv6 reachability. If the NSP does not provide IPv6 access, the Dial-up provider may install additional connectivity to alternate NSP providers of IPv6 reachability to deliver IPv6 traffic or build IPv6 tunnels over IPv4 to reach an IPv6 router which has global IPv6 reachability.

6.4. Traffic Engineering

Traffic Engineering (TE) at the dialup ISP level is closer to connection load balancing. TE is generally done by the authentication servers, which monitor the number of active connections and balance connections across available ISP routed connections.

There are no considerations for IPv6 in terms of traditional traffic engineering in the dialup scenario. There may be a need to balance incoming IPv6 dialup connections across a radius server via a load-balancing switch device.

6.5. Security

Security in the dialup ISP model is mainly meant to protect the network gear from intrusion. By default the terminal servers prevent connections between users.

For IPv6, the Dial-up ISP must determine whether to protect all devices on local segments from being attacked via a native IPv6 transport.

6.6. Network Management

Accounting and statistical information is collected on a per-user basis for billing purposes and the tools required need to support gathering IPv6 data.

6.7. Hosting Gear

There are a number of hosts that support the dialup ISP model. All servers do not necessarily reside at the terminal server point of connection. Servers included in this model include DNS, Radius, and Mail servers that directly support the end user but are deployed in an optimum location. Reachability to the servers is over an IPv4 routed connection. Servers indirectly related to supporting the user include TACACS servers used to authenticate access to network equipment, tool servers to query and monitor, and cache servers that assist in handling web requests. Cache servers are typically used transparently in between the user and the Internet.

The Dial-up ISP must determine which host infrastructure must be reachable via IPv6. The devices in question may include all the servers mentioned above depending on the service offering.

7. Public Wireless LAN

This section describes the infrastructure that exists in today's public wireless LAN services.

7.1 Topology

7.1.1 Physical architecture of public wireless LAN

Public wireless LAN (WLAN) enables subscribers within home, office or the outdoors to perform Internet access by using WLAN technology. WLAN technology is standardized by IEEE 802.11, and its maximum transmission speed varies from 1 or 2 Mbps (IEEE 802.11) and 11 Mbps (IEEE 802.11b) to 54 Mbps (IEEE 802.11a).
Figure 7.1.1 describes the physical architecture of wireless LAN model.

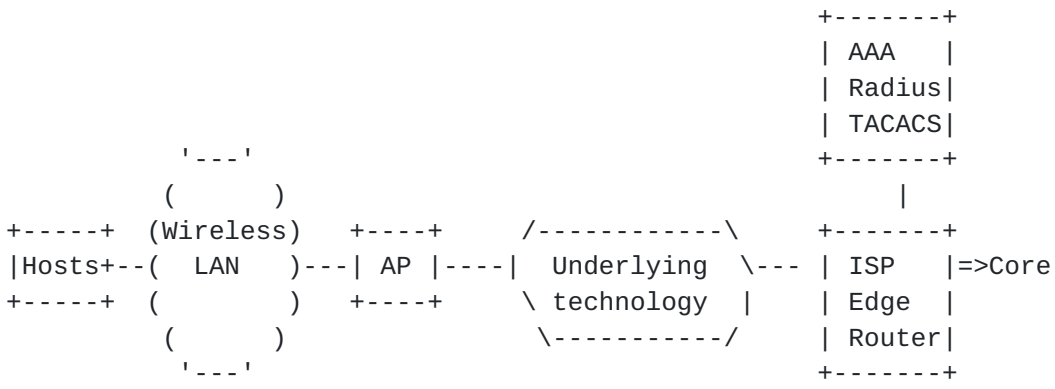


Figure 7.1.1. Physical architecture of WLAN model.

Hosts can connect to WLAN by using WLAN network interface card (NIC), by using PCI or PCMCIA slot. WLAN is basically a broadcast network, and several hosts can share the network by using carrier sense multiple access with collision avoidance (CSMA/CA) access mechanism. Legacy WLAN does not consider authentication and security, but allow any subscriber to connect the network at any time. However, in order for WLAN to be used as public access network, such authentication and security mechanisms are required. Access point (AP) acts as an authentication client, and sends host's authentication parameter to authentication server. Such mechanisms are presented in 3.x.5 in detail. Once the host is authenticated, AP acts as a bridge in order to relay host's information to ISP or vice versa. Various access network technologies can be used between AP and ISP. Lease line, xDSL and HFC/cable are few examples.

7.1.2 Logical architecture of WLAN for data transmission

Figure 7.1.2 describes protocol architecture of WLAN model.

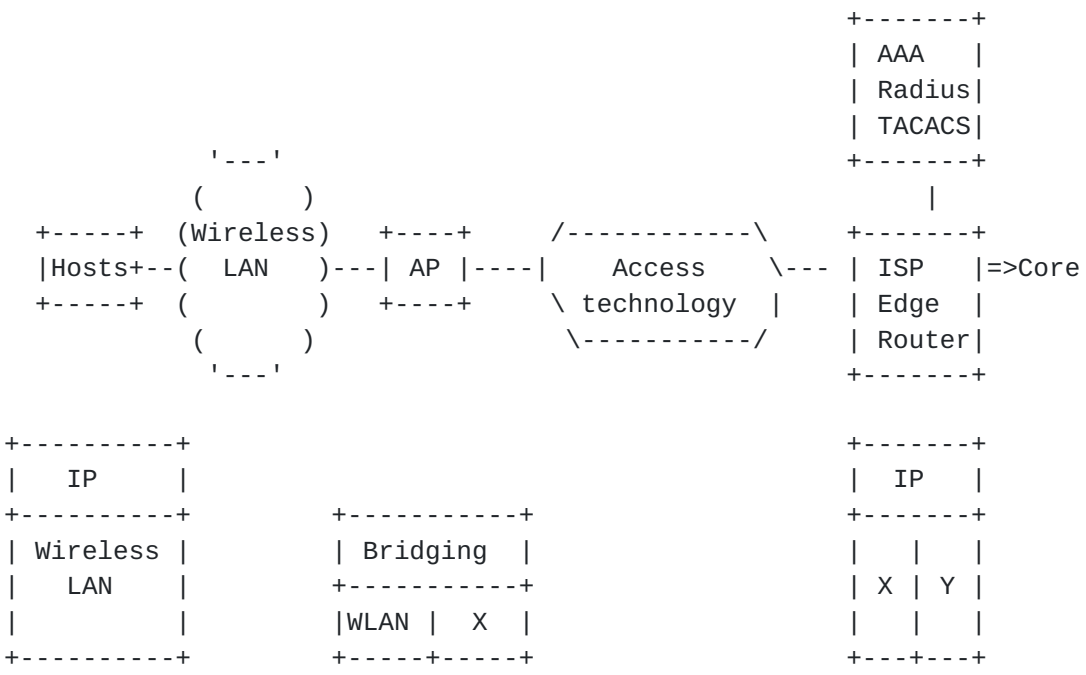


Figure 7.1.2 Logical architecture of WLAN for data transmission
X is subscriber technology (leased line, xDSL, HFC/cable, etc.).
Y is WAN technology (SONET/SDH, ATM, etc.).

7.2 Routing and Addressing

Public wireless LANs are usually configured in small area (aka, hot spots) and basically broadcast networks. Thus, they do not require the use of a routing protocol. One of benefits of public WLAN is to provide for customers convenient Internet access. This allows the customers in the outdoors to connect to public access networks. ISPs supply not static addresses by default but dynamic addresses by DHCP. The customers are usually disconnected every time and are given a new address each time they reconnect. Most of the times, customers use private addressing and the access routers then perform NAT for Internet access.

7.3 Traffic Engineering

ISPs may need to configure traffic filtering or provisioning on demand of their customers.

7.4 Security

Like ethernet, IEEE 802.11 standard dose not define authentication and security mechanisms. Moreover, WLAN is basically a broadcast network and each host can listen information of another host within the same AP service area. Therefore, in order for ISPs to use WLAN as public access network, they should provide authentication and data privacy mechanisms. Authentication mechanism is used to identify whether a subscriber is registered to access the Internet. There can be two authentication mechanisms: (1) IEEE 802.1x and (2) non-standard MAC address based authentication. Once a subscriber is considered as valid, information exchanged between AP and the subscriber should be encrypted in order not to be understood by others. IEEE 802.11i is being standardized on new form of robust security network (RSN) architecture.

7.4.1 IEEE 802.1x based authentication

IEEE 802.1x enables edge devices such as bridge or AP to perform authentication mechanism, and determines whether to allow or block data transmitted by hosts. It uses extended authentication protocol (EAP) as a standard protocol to transmit subscriber's authentication data. Authentication is based of userID and/or password, and packets transmitted by un-authenticated hosts are filtered and dropped by AP

Figure 8.4.1 describes logical architecture of 802.1x based authentication

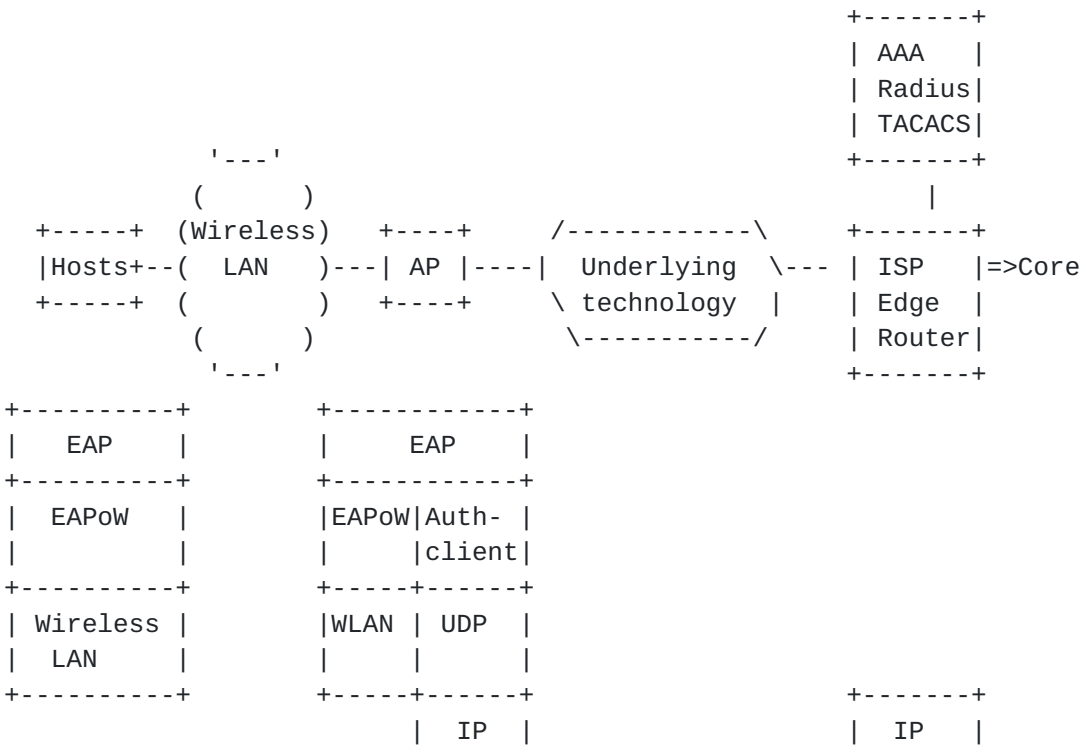


Figure 7.4.1 Logical architecture for authentication

The operation of IEEE 802.11 is as follows. Host trying to access the Internet sends EAP-start message to AP. Then AP requests to host subscriber ID information necessary for user authentication. In this case, subscriber ID follows network access ID (NAI) similar to e-mail address format, in order to support global roaming and accounting. Subscriber ID is inserted in AAA EAP-attribute message and transmitted to authentication server (such as Radius or TACACS server). Finally, authentication procedure is completed when AP receives authentication success/failure message from authentication server.

7.4.2 MAC address based authentication (non-standard)

This mechanism supports host that does not support IEEE 802.1x. In this mechanism, AP inserts MAC address of hosts into username field and sends authentication message to authentication server. The server determines authentication based on MAC address of host. This mechanism can be considered as unsafe method because subscriber can lose the WLAN card and MAC address can be changed.

7.4.3 Data privacy

WLAN is basically broadcast network. Therefore, every host within service area of an AP can listen another host's communication contents. Therefore, very complicated data privacy mechanism must be provided in order not to be revealed by other hosts except intended host. One method to accomplish privacy is to use extension of IEEE 802.1x. Once the subscriber is successfully authenticated, master session key generated during authentication procedure is inserted in authentication success message and transmitted to AP. Then, AP exchanges the key with end host by using EAPoL-key message and synchronizes when to use the key. And then, AP encrypts EAP-success message with the key and sends it to the host in order to notify that the host is allowed to connect WLAN by using IEEE 802.1x. After that, host and AP use dynamically distributed key in order to guarantee privacy within wireless area.

7.4.4 Intrusion Detection, Ingress Filtering, and Prevention

Moreover, intrusion detection, ingress filtering and prevention should be considered.

7.5 Network Management

ISPs manage the edge routers by SNMP. As well, ISPs need the management of AP by means of its configuration tools.

7.6 Hosting Gear

The mail, dns, caching, etc. servers for the customer is usually managed by the ISPs.

8.0 Broadband Ethernet

This section describes the Ethernet based residential access.

8.1. Topology

Physical
The layouts of Ethernet based accesses to the home are all almost identical. They usually consist in a star topology terminated in the apartment building or at a central point in the network. The latter is probably not a common case and is used only for fiber based access. The termination point usually consists of a switch with varying functionality and in some cases a router. At this termination point the network can be connected directly to a metro network or to an aggregation point and a network access server.

Logical
The logical architecture for an Ethernet based access varies but is fundamentally the same. A common practice is to use layer 2 Ethernet VLANs to separate the customers up to the network access server. This is done to assure traceability and prevent eavesdropping by customers as well as to be able to block services such as local file sharing.
User authentication, other than the physical connection, is in some cases used. It can consist of web login or PPPoE. Web login can be done in two ways, one time login where the device's MAC-address is registered and kept or session login where login is done to activate the connection every time the user starts to use it.
The simplest solution is a pure switched network where the users are assigned static addresses and the only controlled device is a router servicing one or several apartment buildings. In this case PPPoE can be used for user authentication if any authentication is used at all.

8.2 Hardware

Routers
Routers are used in the apartment buildings or centralized to control the user traffic in addition to the actual routing. The most common case is to have only switches in the apartment buildings and the routers at an aggregation point since this allows for one router to service several apartment buildings.

Switches
Switches are common in an Ethernet based home access. Usually only layer 2 functionality is used such as Ethernet VLAN.

CPE (router, modem, pc, gateway, appliance, etc)
There is no actual CPEs used if not the actual appliances used by the customer is included.

8.3 Routing

IGP
The interior routing for Ethernet access doesn't differ to any other routing used with in one particular ISP.
The routing protocols normally used are IS-IS or OSPF.

EGP
BGP is used for exchanging external routes.
Exterior routing is not used towards the end customers since the customer networks are seen as being directly connected to the edge router and not having a CPE router in between. This means that the customer network is routed directly to an interface on the edge router and not to a customer router.

Multicast
Sometimes locally enabled to support services like IP-TV. At the moment multicast is not commonly deployed and it is therefore no general way of implementing it.

Addressing
Usually one address is assigned to the user, dynamically by DHCP or statically by manual configuration. Some operators may allow the use of multiple addresses.

NAT
Used in some cases when the operator doesn't have enough addresses.

Aggregation
Aggregation of routes is usually done in several stages in the network.

8.4 Traffic Engineering

Traffic engineering is sometime used in the form of bandwidth throttling. This sometimes adds equipment to the network due to the need of an enforcer. The enforcer could be integrated in the edge router or in a separate entity.
Filtering of traffic is also implemented in many networks mostly as a simple protection of the users or in other cases as a way of preventing certain services such as mail servers.

8.5 Security

Security is usually implemented in the form of Ethernet VLAN to separate the users and to enable traceability. The use of VLAN is then used instead of any form of login since the users can be traced through their VLAN TAG. A database mapping VLAN to IP-address is used to allow historical traceability.
To prevent misuse of addresses anti spoofing is implemented in the network, usually on a per user level to prevent a user from *borrowing* another users address.

If PPPoE is used it provides both user authentication and traceability.
Filtering of well known file sharing ports to prevent unintentional services is used as mentioned earlier.

8.6 Network Management

Usually out of band management is used to configure both routers and switches located in the apartment buildings. This is normally done through a separate Ethernet VLAN. The management tools are more or less the same as in the core network.

8.7 Hosting Gear

DNS is managed by the operator as well as any additional services such as mail and web servers. The latter can also in some cases be run by the customer but for the mainstream user this is not the case.

9.0 Internet Exchange (IX)

This section describes the infrastructure that exists in IPv4 Internet exchanges (IX).
An IPv6 IX, unlike current NAPs, may assign independent long-haul provider addresses, according to [RFC2374]. An organization subscribing such addresses will be able to change long-haul provider without having to renumber.

9.1 Topology

An IX is based on a layer 2 infrastructure that can be, either local to given building, or distributed over a large are by the way multiple interconnected point of presence. This layer 2 infrastructure enables players (e.g. long haul providers) that are connected to the IX to exchange routes.
Figure 9.1a below, describes a typical single sited IX.

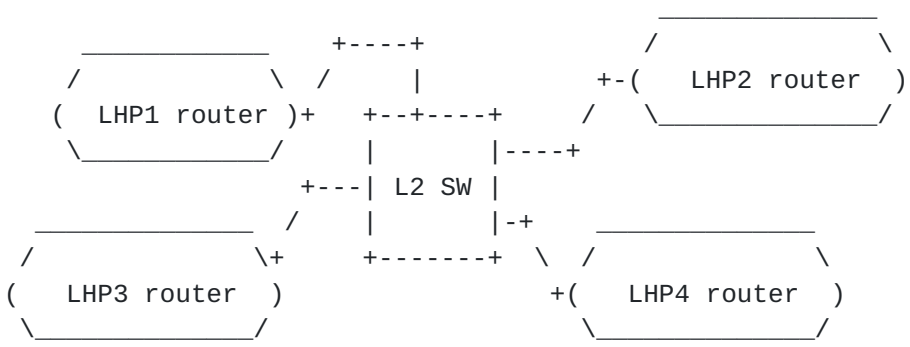


Figure 9.1a

According to [RFC2374] aggreatable addresses are organized into a three level hierarchy. IXs, together with long haul providers, belong the higher one called "Public Topology". IXs will allocate IPv6 addresses to its directly connected subscribers, providing them addressing independence from long haul providers. IX will then have to include layer 3 functions, e.g. by the means of a router, in order to exchange routes with long haul provider, for gaining global connectivity to its subscribers. The figure below, describes such a new type of IX introducing layer 3 functions, and that topology differs from regular IPv4 IX.

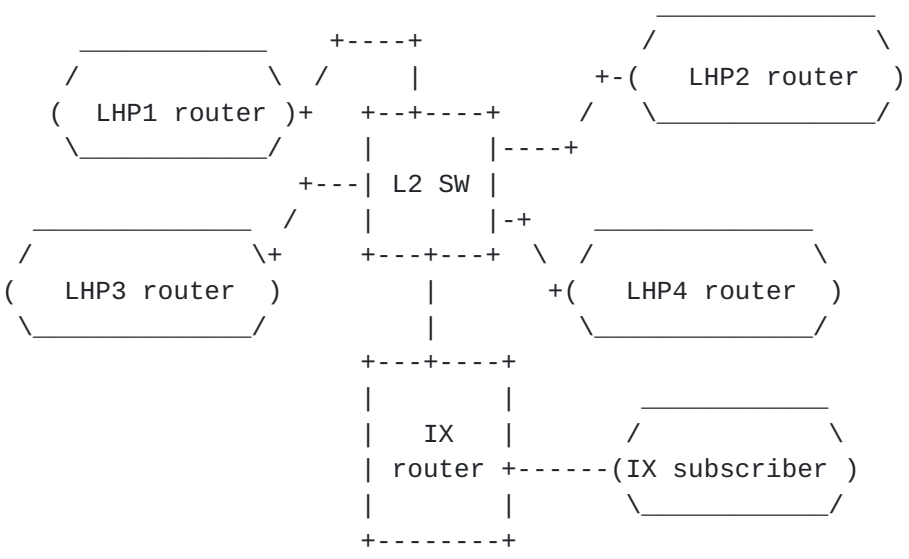


Figure 9.1b

9.1.1 Hardware

Basically, a regular IX is based on a layer 2 switch, or set of layer 2 switches that may either local to a building, or distributed over larger area. It provides also room space and power supply to enable long haul providers to install their own routers and to exchange routes to each other according to a peering agreement.

In the case of an IX providing independent addresses to its directly connected subscribers, the needed layer 3 function will be based on a regular IPv6 router.

9.2 Routing

The main goal of an IX, is to enable long haul provider to exchange routes by the way of BGP4+ peering. An IX implementing layer 2 devices only will not participate to into routing and BGP4+ peering.

An IX providing independent addresses to its directly connected subscribers, will exchange routes with long haul provider by the way of BGP4+ peering.

9.3 Traffic Engineering/Policing

In the case of an IX providing independent addresses to its directly connected subscribers, specific rules may be introduced in order to filter the traffic from a given subscriber to a provider (or a set of provider) according to a given subscription agreement.

9.4 Security

9.5 Network Management

This section does not apply to regular layer 2 based IX, since only local direct peering between third parties is involved.

9.6 Host gear

Do not apply.

10. SECURITY CONSIDERATIONS

Security concerns will be described within the context of each scenario. After the various scenarios are documented, a summarized section including all of the security considerations may be provided.

11. NETWORK MANAGEMENT CONSIDERATIONS

Network Management concerns will be described within the context of each scenario. After the various scenarios are documented, a summarized section including all of the Network Management considerations may be provided.

ACKNOWLEDGEMENTS

[1] The comments from the V6OPS working group are appreciated.

REFERENCES

[01] TR-025 Core Network Architecture for Access to Legacy Data Networks over ADSL, TR-025 - ADSL Forum, September 1999

[02] RFC 1661 The Point-to-Point Protocol (PPP)
[03] RFC 2684 Multiprotocol Encapsulation over ATM Adaptation Layer 5
[04] RFC 2364 PPP Over AAL5
[05] RFC 2516 A Method for Transmitting PPP Over Ethernet (PPPoE)
[06] RFC 2661 Layer Two Tunneling Protocol "L2TP"
[07] RFC 2138 Remote Authentication Dial In User Service (RADIUS)
[08] RFC 3162 RADIUS and IPv6
[09] ANSI/IEEE Std 802.11, 1999 Edition: "Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications".
[10] IEEE Std 802.11b-1999 (Supplement to IEEE 802.11, 1999 Edition): "Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications: Higher-Speed Physical Layer Extension in the 2.4GHz Band".
[11] IEEE Std 802.11a-1999 (Supplement to IEEE 802.11, 1999 Edition): "Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications: High-speed Physical Layer in the 5GHz Band".
[12] IEEE Std 802.1x-2001, "Port-based Network Access Control".
[13] IEEE Std 802.11i/D2.0, "Specification for Enhanced Security", Mar. 2002.
[14] B. Aboba and M. Beadles, "The Network Access Identifier", IETF RFC 2486, Jan. 1999.
[15] P. Calhoun and C. Perkins, "Mobile IP Network Access Identifier Extension for IPv4", IETF RFC 2794, Mar. 2000.
[16] L. Blink and J. Vollbrecht, "PPP Extensible Authentication Protocol (EAP)", IETF RFC 2284, Mar. 1998.
[17] B. Aboba and D. Simon, "PPP EAP TLS Authentication Protocol", IETF RFC 2716, Oct. 1999.
[18] Society of Cable Telecommunications Engineers (SCTE), "SCTE 22-1 2002 DOCSIS 1.0 Radio Frequency Interface", Nov 2001, <http://www.scte.org/standards/standardsavailable.html>.
[19] Society of Cable Telecommunications Engineers (SCTE), "SCTE 23-1 2002 DOCSIS 1.1 Part 1: Radio Frequency Interface", Aug 2002, <http://www.scte.org/standards/standardsavailable.html>.
[20] Cable Labs, "Radio Frequency Interface Specification SP-RFIv2.0-I02-020617", Jun 2002, <http://www.cablemodem.org/specifications/>.

[21] Postel, J. and K. Harrenstien, "Time Protocol", STD 26, RFC 868, May 1983.

[22] Case, J., Fedor, M., Schoffstall, M. and J. Davin, "Simple Network Management Protocol (SNMP)", STD 15, RFC 1157, May 1990.

[23] Sollins, K., "The TFTP Protocol (Revision 2)", STD 33, RFC 1350, July 1992.

[24] Droms, R., "Dynamic Host Configuration Protocol", RFC 2131, Aug 1997.

[25] Fenner, W., "Internet Group Management Protocol, Version 2", RFC 2236, November 1997.

[26] Narten, T., Nordmark, E. and W. Simpson, "Neighbor Discovery for IP Version 6 (IPv6)", RFC 2461, December 1998.

[27] Thomson, S. and T. Narten, "IPv6 Stateless Address Autoconfiguration", RFC 2462, December 1998.

[28] Durand, A., Fasano, P., Guardini, I. and D. Lento, "IPv6 Tunnel Broker", RFC 3053, February 2001.

[29] Carpenter, B. and K. Moore, "Connection of IPv6 Domains via IPv4 Clouds", RFC 3056, February 2001.

[30] Huitema, C., "An Anycast Prefix for 6to4 Relay Routers", RFC 3068, Aug 2001.

TERMS AND ACRONYMS

AAL5 ATM Adaptation Layer 5
ADSL Asymmetric Digital Subscriber Line
BAS Broadband Access Server
CPE Customer Premises Equipment
DSL Digital Subscriber Line
DSLAM DSL Access Multiplexer
L2TP Layer Two Tunneling Protocol
LAA L2TP Access Aggregation (model)
LAC L2TP Access Concentrator
LNS L2TP Network Server
MSS Maximum Segment Size (MTU - 40 bytes for IP and TCP headers)
MTU Maximum Transmission Unit
NAP Network Access Provider
NAT Network Address and Port Translation
NSP Network Service Provider
POP Point Of Presence
POTS Plain Old Telephone Service
PPP Point-to-Point Protocol
PPPoA PPP over ATM
PPPoE PPP over Ethernet
PSTN Public Switched Telephone Network
PTA PPP Terminated Aggregation (model)
PVC Permanent Virtual Circuit
RADIUS Remote Authentication Dial In User Service
USB Universal Serial Bus
VPI/VCI Virtual Path Identifier with Virtual Channel Identifier
VPN Virtual Private Network

Author's Addresses

Vladimir Ksinant
6Wind
1 place Charles de Gaulle - 78180 Phone: +33139309236
Montigny Le Bretonneux - France Email:vladimir.ksinant@6wind.com

Jae-Hwoon Lee
Dongguk Univ.
26, 3 Pil-Dong, Chung-gu, Phone: +82 2 2260 3849
Seoul 100-715, Korea Email: jaehwoon@dgu.ac.kr

Myung-Ki Shin
ETRI PEC
161 Kajong-Dong, Yusong-Gu, Phone: +82 42 860 4847
Taejon 305-350, Korea Email: mkshin@pec.etri.re.kr

Aidan Williams
Motorola Australian Research Centre
Locked Bag 5028 Phone: +61 2 9666 0500
Botany, NSW 1455 Email: Aidan.Williams@motorola.com
Australia
URI: http://www.motorola.com.au/marc/

Alain Baudot
France Telecom R&D
42, rue des coutures Phone: +33 2.31.75.94.27
BP 6243 Email: alain.baudot@rd.francetelecom.com
14066 Caen, FRANCE

Mikael Lind
Telia Research
Vitsandsgatan 9B
123 86 Farsta Phone: +46 70 2406140
Sweden Email: Mikael.e.lind@telia.se

Cleveland Mickles
America Online, Inc (owned by AOL Time Warner)
12100 Sunrise Valley Drive. Phone: +1 703-265-5618
Reston, VA 20191, USA Email: micklesc@aol.net