2 Introduction

A traditional cable company operates a network designed to deliver high-quality television signals to subscribers in a well-defined franchise area. The operator obtains video program feeds from multiple sources utilizing satellite, local origination, and land-line technologies. These various video sources are combined into 6MHz channels to be sent to customers over coaxial cable or hybrid fiber-coaxial (HFC) cable network systems. This is directly analogous to over air broadcast with the air replaced by a wired network.

Two-way enabled plants are capable of delivering signals upstream, from the home towards the head-end. The original motivation for deployment of two-way plant was to enable services such as Impulse-Pay-Per-View.

With the availability of two-way plant other bi-directional services are possible. In particular, data and voice communication that use Internet Protocol (IP) technologies. The technology used to build the cable TV distribution plant is well suited for high-speed delivery of data services. The channelized physical media is capable of carrying 100+ separate information streams downstream (towards the consumer). Each channel is 6Mhz wide and is currently capable of carrying traffic up to 40MBs. Upstream bandwidth is somewhat more constrained. It is carried in the low end of the cable radio frequency (RF) spectrum (5-42Mhz) and must compete with a broad range of other signals, much of which appear as noise. Upstream data is typically channelized in spectrum slices from 0.1 to 4 Mhz, resulting in digital data rates from 128Kb/s to 10Mb/s.

2.1 Generic End-to-end High-speed Data Service

Carrying High-Speed Data (HSD) or other baseband packet-oriented services over HFC infrastructure is conceptually simple. Downstream and upstream channel space is assigned and equipment is installed that converts and modulates baseband digital signals into the RF frequency range. The cable industry has defined the Data Over Cable Service Interface Specification (DOCSIS) standard that specifies interfaces and architectures for HSD over the cable HFC plant [see: http://www.cablemodem.com/]. In the cable company head-end, Cable Modem Termination Systems (CMTSs) are interconnected to wide-area networks on one side and to the HFC on the other side. The CMTS terminates the physical and link-level protocols over the HFC and provides standard interfaces for the transport of traffic on the data network side. Customer premises equipment consists of Cable Modems (CMs) which convert the incoming RF to baseband and typically provide a 10BaseT connection to a subscriber PC. For traffic from the customer PC upstream to the head-end the roles are reversed[1].

[1] Some cable plants are not capable of 2-way operation so the return channel from the consumer PC is carried over a dial-up connection through the PSTN.

It is important to emphasize that HSD traffic is carried in the same physical media as other cable programming services. Different services are distinguished by the frequency bands which they occupy in the media. RF signal quality (hence effective data carrying capability) issues affect all carried services.

Figure 1 depicts the software and hardware systems involved in providing a HSD service over a Cable plant. The transport technologies involved at transition points in a HSD service network are also indicated.

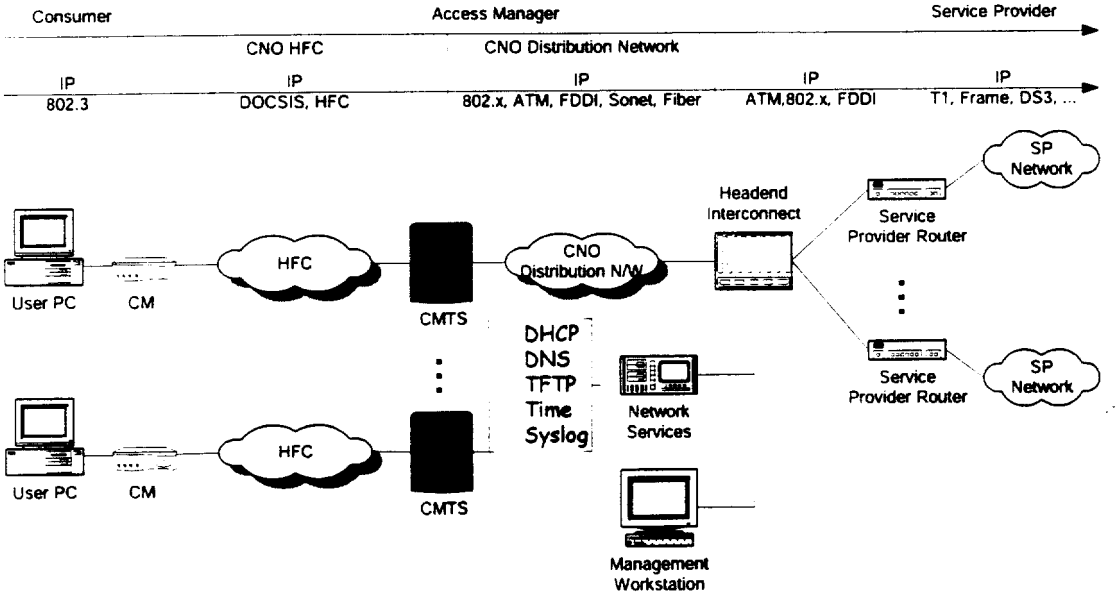

Figure 1 – Generic HSD System

2.2 Who the players are

There are a number of different services provided over the HFC plant. The core cable business is delivering television programming from multiple, independent content providers such as Discovery Networks, A&E, Turner Networks, CBS, etc.. This capability is very easy to provide since there is no return communication or consumer dialog to these providers. In this simple scenario, there are Video Service Providers (A&E, etc.) and the Cable Operator that delivers the content.

Delivery of modern IP-based data services is more complicated than providing simple broadcast of television signals. Even in a small LAN environment as might be found in a small office, design, implementation, management, and maintenance of the data services are outsourced to experts in those services. Cable operators that offer data networking services must install Metropolitan Area Networks involving technology and skills at physical, link, and network layers. High-speed Data services (HSD) require addition of a provider of IP services to support the basic layer three and above network and system management services.

The view taken here is illustrated in Figure 2. This identifies three parties:

1. Cable Network Operator (CNO) - owns the HFC plant infrastructure, maintains a force to service those facilities and provides channel space and connection points to that RF environment. In addition, the Cable Operator might own and maintain a distribution fiber network within its franchise area to deliver programming to its HFC access network. The Cable Operator may or may not own the IP networking equipment.

2. Access Manager (AM) - Manages the local (or regional) IP networking service. They are responsible for Layer 2 and 3 network configuration, and management in the Access Network. The AM may have designed the IP network layered over the Cable Operator's plant. Also, the AM will be responsible for basic IP networking services that enable traffic to flow. The AM may or may not own the IP networking equipment.

3. Service Provider (ISP) - Manages the global IP networking service. The ISP has a direct relationship with the end-customer to provide content applications, and support services (e.g. help desk). The ISP manages its pools of IP addresses and provides session authentication for its customers. There may be multiple ISPs of multiple services.

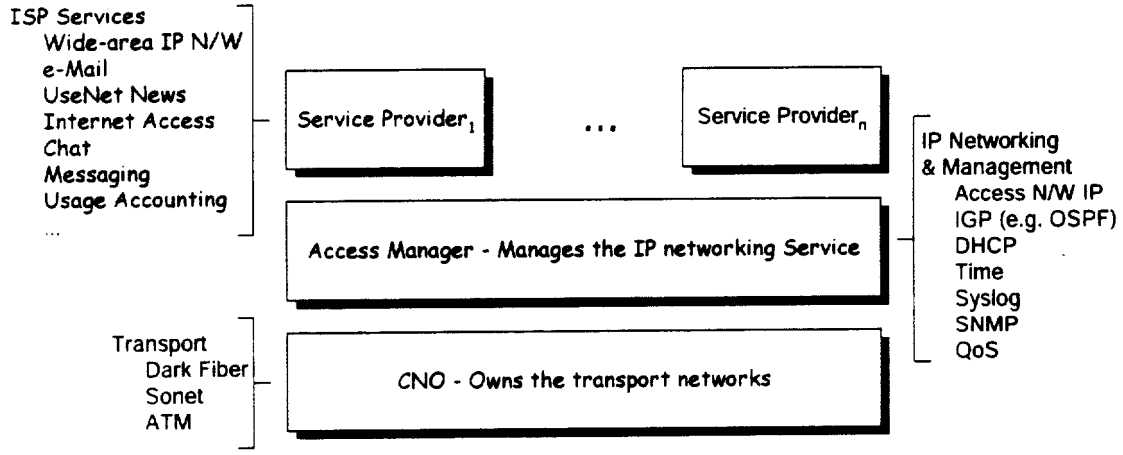

Figure 2 – Relationships among providers in a HSD system

The distinctions are clearly delineated with each layer offering services to the group above it. Cable Operators provide raw bandwidth to AMs. AMs create packet delivery services with varying bandwidth and Quality-of-Service (QoS) guarantees. ISPs present services to consumers such as e-Mail, web access, content, etc.

Consumers have responsibility for the CPE equipment that connects them to the access network. Consumers may call their ISP for assistance when there are problems. AMs deliver consumer traffic to the multiple ISPs. Later sections will detail the requirements for this service[2].

[2] The functional separation between Cable Operator and Access Manager is useful to define the technical and operational requirements. It is possible that both organizations are merged in a single entity, as a

business decision, while the functional separation assumed here is still applicable.

AOL(2)001851

3 Definition of Equal Access

Equal Access is intended to provide open interfaces and processes for the proper end-to-end service delivery from multiple ISPs to consumers over shared media. Equal Access does not confer unfettered rights to any of the participants. There are three main assertions of Equal Access:

- Equal opportunity for consumers to choose their ISP. Consumers are able to obtain services from any ISP that has a presence in the access network.
- Equal opportunity for multiple ISPs to reach all consumers over common access infrastructure with differentiated service offerings. The ISP controls and is responsible for delivery of content, applications, and IP networking services to and from a demarcation point within the access network provided by the AM.
- There is no cost, service, or performance discrimination to the consumer for exercising their choice of ISP. To clarify this further, the consumer incurs no penalty (either cost or performance) to unbundle access from service. Consumers only receive the services they want to pay for, and only pay for the services they want to receive.

3.1 Consumer-Oriented View

Consumers can only have a choice if there are multiple ISPs available through the access network to which they connect. Given that there are multiple ISPs available, consumers are allowed to choose their ISP irrespective of Cable Operator or AM preference for ISP. If Cable Operator is also an ISP, all other ISPs must be able to obtain the same equitable terms as the Cable Operator ISP. This prevents the Cable Operator from disadvantaging ISPs.

The Cable Operator cannot force the consumer to accept additional ISP services to get the ISP of consumer's choice. Consumers should not be forced into a bundle of access and service in addition to the cost of their preferred provider. This ensures consumers are not disadvantaged by a need to pay for the Cable Operator's ISP as well as their chosen ISP.

Req 1. The AM **must** provide one or more IP transport classes that are available to all ISPs on equitable terms.

A class of IP transport is delivered to an individual modem and includes configurable items such as maximum and minimum downstream and upstream bandwidth, latency, etc. Other configuration items that will be incorporated into IP transport classes (or tiers) will be, for instance, the number of CPE allowed and number of IP addresses that can be configured to consumer CPE.

AOL(2)001852

3.2 Technology-Oriented View

ISPs require the ability to directly interconnect its network with that of individual Cable Operators that offer HSD services. The interconnect supports bi-directional, layer 3 (IP) traffic flow for ISP customers on the Cable Operator's cable network. The AM is responsible for managing the infrastructure and equipment necessary to ensure reliable layer 3 (IP) transport between ISP customers and an agreed upon demarcation point with the ISP network.

Req 2. The AM **must** provide an interconnection interface to its distribution network at points where all of the ISP's traffic aggregates.

The access model need not be inflexible. In fact, AMs must be granted latitude with respect to implementation, and the ability to utilize software and hardware technology improvements provided the necessary functionality is met. For example, an AM may grant access through one or more technologies, including but not limited to shared media (e.g., ethernet), dedicated synchronous connections (e.g., DS1 or DS3), or other standardized interfaces (e.g., ATM). Demarcation points may be chosen to avoid any ISP ownership of equipment at the Cable Operator location, or a co-location agreement may be desirable. Similarly, the AM may define multiple physical interconnection points to provide for redundancy or scalablity.

The AM network between the consumer's CM and the ISP interconnection point can be either a routed or bridged network design. Each of these has different IP address allocation strategies for network elements, and different requirements for network element configuration. The AM will implement an efficient modem IP address allocation and management design that does not place an undue burden on address pools or access strategies.

DOCSIS modems are addressable network elements for management and service provisioning purposes. They acquire IP addresses and require system resources (detailed in Section 3) to operate. AMs will need to make choices in address plan design that do not conflict with possible Equal Access address plans for consumer's CPE, or unnecessarily deplete the ISP's address space. AMs should not require more than a single Internet-routable IP address to be allocated per consumer CPE.

Whenever possible, AMs should use non-Internet routable address blocks for network elements, CMs, and Consumer PCs. However, the AM is constrained to implement a CPE address space allocation and management policy consistent with the network system design and process flows at a particular Cable Operator location.

The AM must permit the management of individual, disjoint IP address blocks among customers of all ISPs, including the Cable Operator/AM itself. A Cable Operator/AM may require ISPs to supply the IP address block for customer use, or it may choose to sub-allocate such blocks from a larger pool of its own.

Requirements for address blocks vary depending on the technique used for traffic separation and the design of the AM IP network. In general however, if the ISP point-of-interconnection (POI) is outside of the AM

IP network, addresses assigned to consumer PCs will need to be chosen from routable address blocks. When the ISP POI is inside the AM IP network, address blocks can be non-Internet routable.

When the ISP is required to supply Internet routable addresses, they will need to do so in accordance with existing conventions. In particular, many peering arrangements require address blocks with at least /19 prefixes to facilitate route distribution. The ISP in this case would need to supply at least 32 contiguous Class C address blocks to the AM for use by the ISP's customers PCs to ensure proper Internet connectivity.

Req 3. The AM **must** create and maintain network element configurations that implement the IP transport classes offered to the ISPs.

This includes DOCSIS modem configurations, Router, and IP switch configurations. All ISPs must be given access to all QoS (or CoS) definitions that are created and provisioned to particular CMTSs managed by an AM. This is fundamental to Equal Access. All ISPs have equal opportunity to provide equivalent services to their customers and to compete with each other on price or service bundling.

3.3 Consumer Business Relationships between the Parties

There are three models for the business relationship that a consumer might have in order to receive the service of their choice through an HSD-enabled Cable Operator. The business relationship is concerned with two principal process flows. The first is how service ordering and billing are managed, e.g. whether the bill for service comes from the Cable Operator, AM, or both send a bill. The other flow is more extensive and relates how the consumer's service is managed at a network, application gateway, trouble resolution, and provisioning level.

In general, AMs, ISPs, and Cable Operators should implement processes and procedures to efficiently notify each other of new or departing consumers, changes in consumer service levels, and initiate and track trouble calls. The need is clear to log consumer's requests for service and to have means to evaluate both ISP and AM performance in satisfying requests. ISPs and AMs must create a mutually agreeable way to record and manage service changes requested by consumers.

The three consumer business models considered are described in following sections.

3.3.1 User deals with ISP

In this scenario, the User orders service and expects service fulfillment from the ISP. The ISP then needs to negotiate with the Cable Operator and the AM to arrange for installation (if needed) and for IP connectivity.

This model has the User interacting directly with the ISP and expecting guarantees at that level. The ISP receives trouble calls first. In contrast with service-level problems (e.g. missing e-mail), if there is

a performance problem related to the local access network, the ISP may have to contact the Cable Operator/AM to determine the nature of the problem or have visibility into the Cable Operator/AM management systems. Service Level Agreements will be in place between the Cable Operator/AM and the ISP to ensure appropriate levels of customer satisfaction.

3.3.2 Consumer deals with Cable Operator or AM

This is another single-point-of-contact model, where the consumer deals with the Cable Operator/AM directly. When the consumer requests HSD service through the Cable Operator or AM they are presented with a selection of ISPs that offer services in that franchise. The Cable Operator or AM is responsible for service fulfillment. The consumer selects an ISP from a menu. The Cable Operator or AM arranges the installation (if needed) and IP connectivity, and alerts the ISP that another customer is coming in their direction.

Alternatively, the Cable Operator/AM could hand-off the consumer to the ISP once activation is completed, and the model then follows Section 2.3.1 after the initial provisioning.

Trouble calls would be first handled by the Cable Operator or AM help desk. If it is determined that the caller's problem is not related to the local access network, the Cable Operator/AM may have to contact the ISP to determine the nature of the problem or have visibility into the ISP management systems. Service Level Agreements will be in place between the ISP and the Cable Operator/AM to ensure appropriate levels of customer satisfaction.

3.3.3 Consumer deals with AM and ISP

This model is the most complicated for the consumer to manage. They would need to arrange IP transport from the AM or Cable Operator and then go to the ISP to arrange for Application Gateway services. It is possible that multiple service fulfillment appointments might need to be scheduled and that multiple bills would need to be dealt with.

3.4 AM – ISP Relationships

Figure 3 illustrates the relationships between the AM and ISP. The AM is in the business of providing IP transport to the ISP. The Service - Transport maps define these relationships. The structure of these relationships ultimately determines what the consumer's ability to choose is. There are at least four mappings that must be managed to provide consumers with a pleasant Internet experience.

1. Packet Delivery - determines how the consumer's traffic is routed to their ISP. Traffic destined for a particular ISP must be delivered from and to the AM with as much efficiency as possible.
2. Service Ordering and Activation flows - determine how the consumer requests and has services activated for use.

3. Trouble Reporting, Diagnosis, and Repair - determine how the consumer deals with problems with service access or apparent problems with the services they expect to receive.

4. Billing - determines how the various parties pay each other for the services they obtain.

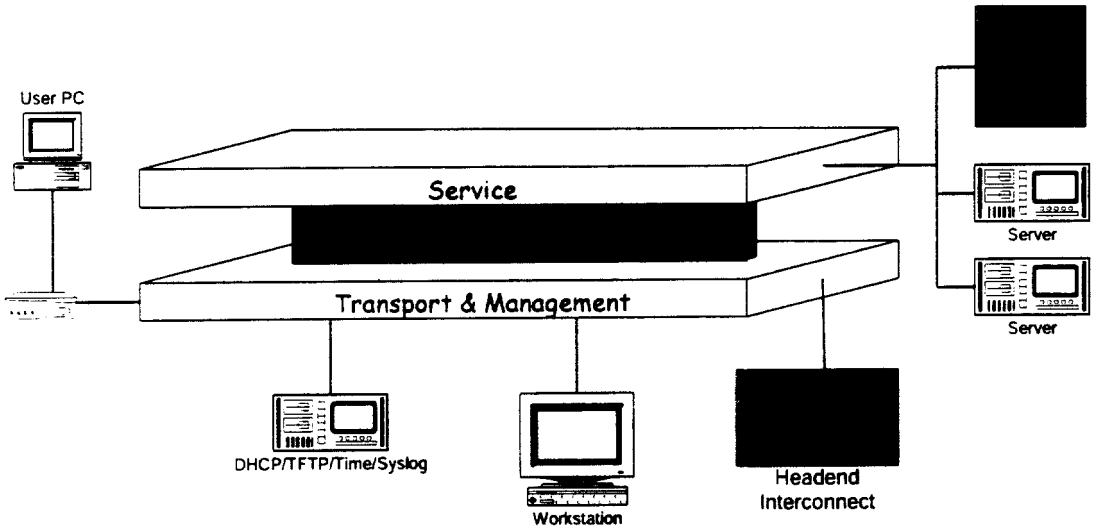

Figure 3 - ISP-AM relationships

In order to create a trouble-free Internet experience for consumers and provide maximum efficiency for Operations and Business Support Systems (OSSs), these relationships must be automated as much as possible. Important functions such as logging initial service requests, service change requests, and trouble reporting are particularly important to be automation accessible.

AOL(2)001856

4 Requirements for System Architecture

This section will discuss various schemes for access that connect consumers to the ISP of their choice. A simple set of role definitions is in order. The Cable Operator is responsible for physical connectivity both of the consumer to the AM (through the HFC) and onto the AM Traffic Aggregation point (generally the headend).

The AM is responsible for transport of all service-bound IP packets from the CM attached to a consumer's PC to the preferred ISP. The AM must give all ISPs non-discriminatory efficiencies in transport based appropriate IP transport classes. The AM needs to manage the common access infrastructure (owned by the Cable Operator) to provide reliable IP transport from the consumer to an ISP aggregation point. The AM is responsible for configuration of all network elements used to provide transport from consumers to ISPs.

The AM will generally have a management system that controls Network resources and has visibility into all attached equipment. The ISP does not necessarily have visibility into the AM's network under normal conditions and so must rely on agreements with the AM to ensure proper system management.

Req 4. The AM **must** route consumer traffic to and from their chosen ISPs so that each ISP can manage IP address space for its service and route service-bound IP traffic for its customers. The AM will either separate consumer IP traffic destined for different ISPs, or provide mechanisms to allow ISPs to implement access controls.

This is a key provision of Equal Access. It allows each ISP to treat its customers in a uniform manner. AMs will not need to manage multiple diverse address spaces. ISPs will be responsible for all service resources allocated to individuals (e.g. Internet-routable address spaces).

The goal is to allow consumers to only obtain services that they have contracted for. One way to accomplish this is for the AM to employ schemes that avoid sending traffic flows of one ISP to any other ISP when they reach ISP aggregation points. An important implication of this requirement is that some combination of tunnelling techniques or physical separation of traffic is necessary. Another way is for the AM to confine traffic to its local area and the ISPs to implement access controls on their services at each POI.

Peering agreements between ISPs should be made outside of the AM network. Peering agreements between ISPs may permit their subscribers to communicate in more efficient ways than through the general Internet. ISPs cannot expect AMs to provide facilities within their systems to effect these arrangements since they are outside the scope of these requirements. AMs may opt to do so, however all ISPs must be given equal opportunity to participate.

4.1 Routed and Bridged Network Designs

IP delivery networks can be divided into two broad categories: routed and bridged networks. Bridged networks operate on Layer 2 addresses and provide a continuous Layer 3 address space over a set of interconnected network elements such as IP switches, bridges, and hubs. Routed networks contain multiple routers that interconnect Layer 2 networks and select traffic routes based on Layer 3 addressing and routing protocols. There are Equal Access architectures applicable to either bridged or routed networks.

A routed network is characterized by the interconnection of two or more Layer 2 networks (each a separate MAC domain) by a Layer 3 router. Each segment defines a different IP address space (network number, broadcast Address, Subnet mask, and address list). This is illustrated in Figure 4. Routers employ routing protocols such as OSPF and RIP to exchange connectivity information about the segments.

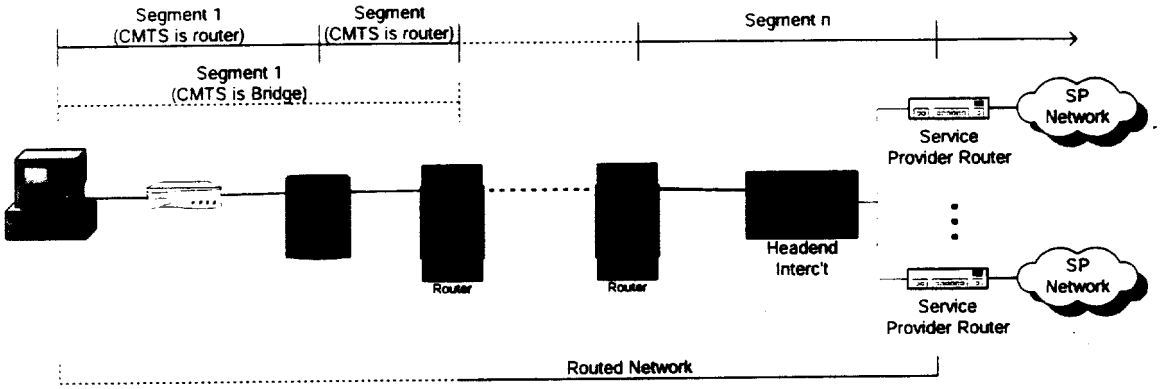

Figure 4 – Routed network model.

A CMTS can be a bridge device (e.g. Nortel CMTS 1000) or act as a router (e.g. Cisco uBR72xx). Figure 4 illustrates both styles of design. If the CMTS is a bridge device, the PC-CM-CMTS is in a single bridged network connected to a router for WAN or MAN connectivity. When the CMTS is a router, individual subnets are usually created for a single downstream transmitter (and its related upstream receivers). The distinguishing feature of the routed network model is that it always includes multiple router hops from Consumer PC to ISP router.

In a bridged network design, all attached elements communicate in a completely connected Layer 2 address space (with some optimizations for address learning by network elements or separation into virtual networks). All network elements are simple hubs, bridges, or addressable elements. Networks of this type implement Layer 3 (IP) address spaces. Figure 5 illustrates this. Asynchronous Transfer Mode (ATM) and Fiber Distributed Data Interface (FDDI) are examples of bridged distribution network technologies.

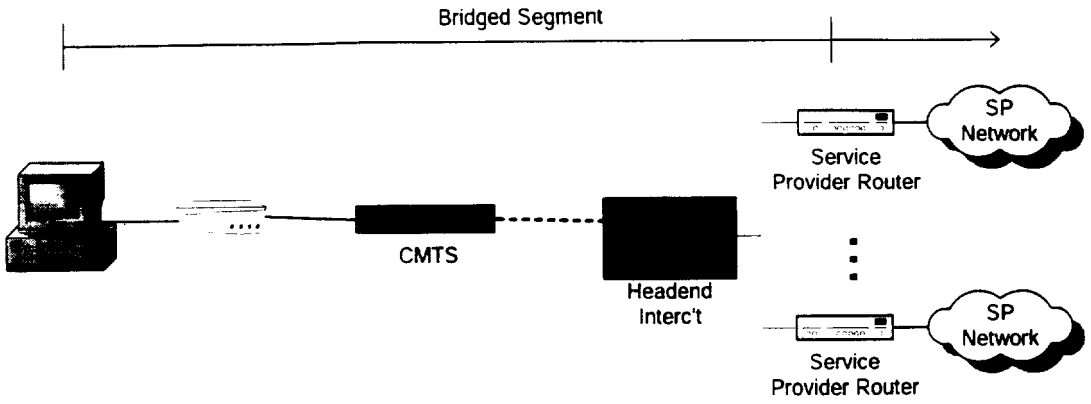

Figure 5 - Bridged distribution network model

Each design class affects important configuration and design elements for the underlying transport system.

- CPE address allocation plan can be different depending on the distribution network design that is chosen.
- The techniques employed to satisfy Requirements 4.
- CM configurations will have varying service provisioning elements and possibly a different CM addressing scheme.

These items will be addressed in later sections.

4.2 Access Network Design Options for Equal Access

The network design to support Requirement 4 might be accomplished in several ways. Each solution will have favorable and unfavorable features. All solutions require service provisioning on a per user or account basis. Following sections will discuss technical issues that affect the choices among these techniques. Many of the issues below relate to unauthorized access to services. While malicious users will intentionally attempt to overcome unauthorized access and indirectly create problems for legitimate users, more widespread concerns are expected with well-intentioned, but clumsy users.

4.2.1 RF Overlays or Channeling

RF overlay networks involve separation of traffic bound for different ISPs into separate RF channels from CM to a channel aggregation point (generally a CMTS). At the channel aggregation point, the traffic is directed to the ISP's point of presence using either a separate CMTS for each ISP, or policy-based routing or tunneling through a shared CMTS.

This approach is limited by the available channel space, and the problems associated with management of the RF plant. At least N + 1 channels downstream will need to be provided. There is a channel for each ISP's downstream traffic, as well as a " hailing channel" that modems must listen to in order to find the channel they are assigned based on ISP. In the upstream direction, many more channels are

AOL(2)001859

required to segregate traffic as well as provide the fiber node combination necessary to provide adequate upstream bandwidth utilization.

Frequency agility considerations and the operational overhead of managing this multiple channel scheme probably make this impractical for implementation when there are more than a few ISPs. This scheme is not recommended, and will not be further discussed in this document.

4.2.2 Policy-based Routing

Policy-based routing is a technique that makes routing decisions based on the characteristics of packets other than their destination address. In a simple form of policy-based routing, a particular consumer's outbound IP traffic is identified by the source address of their PC and directed to a specific next hop or gateway irrespective of normal routing considerations.

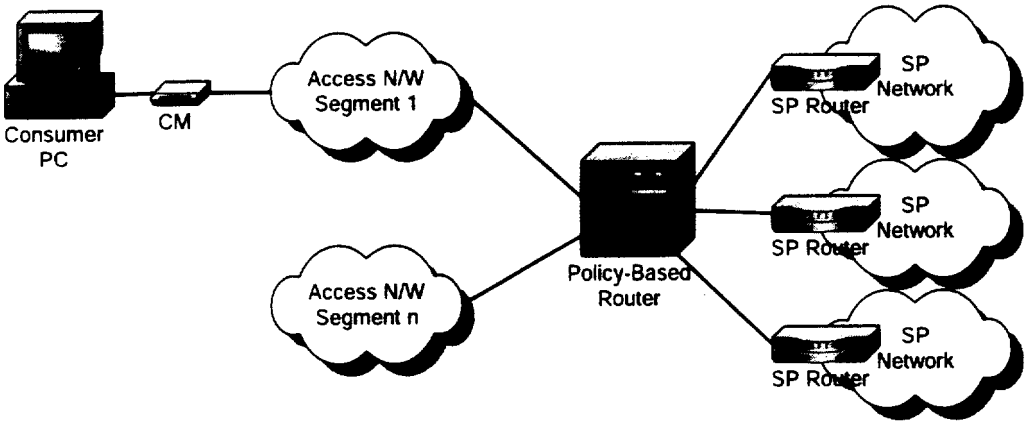

Figure 6 – Policy-based router model

PBR's used to join multiple access network segments effectively implement a physical traffic separation from consumers to ISPs. Clearly, the AM must continue the physical separation or the ISPs must create tunnels to their service networks from the PBR.

In a bridged network design, the policy router must be at the aggregation point of all access network traffic.

Routed networks require that all routers act as PBRs. If not, users will be free to move traffic along any reachable route in the access IP network. When the routed network includes additional routing segments between the first-hop router and the ISPs, the policy must be implemented in each router, or tunnels must be created from the policy routers to provide necessary traffic separation. These items are a consequence of the " Routing Fish" phenomena discussed briefly in Appendix 1.

Policy routing is an effective technique when all traffic must pass through a common point from which it can be directed to the appropriate

ISP. Several design points, including overall network design and address space allocation mechanisms limit the applicability of Policy Routing. Current Policy Router implementations only permit specification of either a next-hop address or a specific point-to-point interface on which to deliver traffic. Binding a particular consumer to a policy will depend on the implementation of the policy classification and how the consumer is identified to the system. Source addressed-based techniques will require either static IP address bindings, or dynamic policy creation and distribution.

A pure policy-based router solution is probably most appropriate when the Cable Operator is small, with distribution hubs co-located with a headend. The PBR solution is also appropriate when the AM distribution network is implemented as an ATM or FDDI network.

4.2.3 VPNs and IP Tunnels

A Virtual Private Network (VPN) connects the components and resources of one network over another network, called the transit internetwork. VPNs accomplish this by using techniques that allow users to tunnel traffic through the transit internetwork. The service-bound payload to be transferred is encapsulated in a frame or packet of the transit internetwork for transport through the intermediate network.

VPNs can be created at many levels of the protocol hierarchy and encapsulate traffic in many ways - some more efficiently than others. Important factors to consider are how the tunnel is established and maintained, and what services the encapsulated protocol receives from the surrounding protocol.

IP tunnels work by establishing an IP connection from one tunnel endpoint to a tunnel server through the transit internetwork (Figure 7). IP packets delivered from the endpoint are encapsulated in IP packets of the transit internetwork and sent to the tunnel server. At the tunnel server, the packet is unencapsulated and sent to its intended destination. L2TP [RFC2661] and PPTP [RFC2637] are both readily available tunneling technologies implemented by a number of vendors.

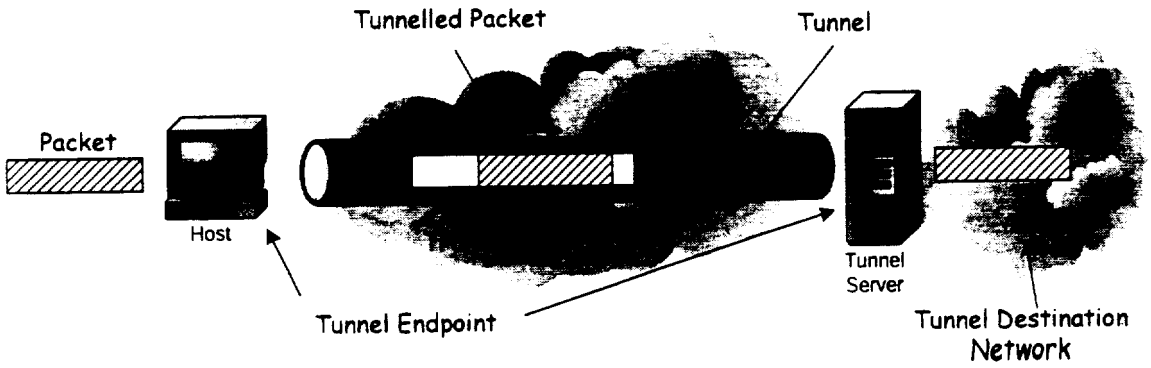

Figure 7 - Tunnel terminology

In an Equal Access implementation, each ISP would connect a tunnel server at the headend or regional interconnection point. Each ISP could

choose their own techniques for authenticating and authorizing their customers. They also must choose a technique to deliver traffic from the tunnel server to their destination network. The tunnel server might be directly connected into the ISP network through a local point-of-presence. Alternatively, the tunnel server might form the start of another tunnel through another shared network (such as the Internet).

The tunnel IP connection exists in the address space of the transit internetwork. Both the Host and the Tunnel server require addresses routable within the transit internetwork. However the tunneled packet source address is allocated from the address space of the tunnel destination network.

Individual consumers would create a tunnel to their chosen ISP server and send all of their service-bound packets through the established tunnel. In this scheme, an individual consumer uses an L2TP or PPTP - enabled protocol stack to establish the tunnel. Each service-bound consumer packet is encapsulated in a packet directed at the tunnel server. The tunnel server extracts the original payload packet and routes it through its egress interface.

4.2.4 PPPoE encapsulation and Policy-based Routers

Another tunneling technique uses Point-to-Point Protocol over Ethernet (PPPoE [RFC2516]) to connect hosts over a bridged network to a Remote Access Concentrator (RAC). The RAC serves the same function as the tunnel server in IP tunneling solutions. In this case the host locates and establishes a session with the RAC. Service-bound packets are encapsulated in PPP [RFC1661] frames and unicast at the link level to the RAC.

Implementing this solution to satisfy Requirement 4 requires a bridged network and combines tunneling at Layer 2 with policy-based routing techniques. The RAC could terminate tunnels for multiple ISPs and allow traffic to be policy routed after de-encapsulation. Using PPPoE enables each ISP to assign and manage the IP addresses for their customers. By way of contrast, the pure policy-based technique requires routable addresses managed by the AM.

As with IP tunneling, a special protocol stack is required on the Consumer's PC to create the necessary encapsulation and there are several commercially available implementations (e.g. NTS, RouterWare). Users establish an authenticated connection to the RAC and deliver all of their payload traffic through the connection.

4.3 Establishing IP Connectivity in DOCSIS Networks

All of the techniques and protocols used to implement Equal Access over DOCSIS networks must work within the confines of this definition. DOCSIS specifies a set of standards for delivering packet-based protocols over HFC networks. DOCSIS requires a certain amount of operational support in terms of Network Services, careful system design, and resource management. A consequence of DOCSIS is that AMs will need to create and efficiently manage at least three items:

- The modem address plan. DOCSIS modems are addressable network elements for management and configuration purposes. The AM will create a management address space containing all of the network elements they are responsible for from a large non-Internet-routable address space.
- Service definitions. From the DOCSIS perspective, these are largely bandwidth and scheduling specifications that are tailored to different types of services.
- Modem Configuration files. The detailed parameter settings for services, and the overall configuration file management scheme will be an important consideration in efficient service delivery. Parameter settings are a combination of tag-length-value entries and SNMP MIB variables[DevMIB,RFMIB].

There are currently two DOCSIS standards to be considered: V1.0 and V1.1. DOCSIS V1.0 established the basic and fundamental operational parameters for DOCSIS systems. DOCSIS V1.1 extends the V1.0 specification in significant ways. The most obvious and important extension is a very elaborate and capable set of Quality of Service (QoS) mechanisms. V1.1 also generalizes the concept of a service flow between CMTS and modem, and ties these to QoS. V1.0 by contrast defines a very simple, data-rate-oriented Class of Service (CoS) and only requires a single service flow between CMTS and modem. All V1.0 equipment can be upgraded to V1.1 via software download, and is interoperable with V1.1 equipment.

Consumers will acquire modems in different ways. Loans, rentals, and retail channels are among the possibilities. The DOCSIS standards have been established to enable interoperability of modems - generally a DOCSIS-certified modem is capable of interoperating with any DOCSIS-certified CMTS. DOCSIS certification should be a requirement for a Consumer's modem to be put in service in the Cable Operator location. And, the AM may establish a list of CM vendors and types that it will support in connections to the access network.

The following sections outline the steps involved in initializing a DOCSIS modem and bring it to an operational state. Once fully operational it may allow attached CPE to pass traffic according to the configuration that is loaded.

4.3.1 Establish physical and MAC connectivity

Upon power-up, the modem initializes itself internally and attempts to acquire a downstream channel. Once it finds a usable downstream, the CM will obtain transmit parameters and perform ranging to set its delay characteristics. This step creates needed connectivity and has no useful service-related parameters that can be managed.

4.3.2 Establish IP connectivity

The CM is able to move packets over a temporary service identifier obtained during ranging. At this time it will broadcast for DHCP servers to supply its basic IP configuration and reference to a TFTP server from

which to obtain operational parameters. The CM will contact one of the Time [RFC868] servers to establish an accurate time-of-day.

Req 5. The AM **must** provide a DHCP service from which CMs acquire their IP configurations and RFC868 Time servers which modems use to acquire the current time-of-day.

The DHCP service provides a common, well-managed place for CMs to obtain their IP configuration. Individual CMs can be identified by their MAC addresses. DHCP can use this to supply IP parameters appropriate for the CM. The configuration supplied by the DHCP service allows the CM to locate all of the services necessary for it to become an element in the network and locate its specific set of parameters and configurations.

Time service is required by DOCSIS modems so that they can set their clock to a locally accurate standard. This provides a capability to time-stamp events that are generated as the modem operates.

4.3.3 Transfer configuration file (operational parameters)

The CM has acquired IP parameters and is capable of contacting IP-based servers, but is not yet configured for consumer services. The CM must contact the TFTP server to obtain a configuration appropriate for the set of services that have been contracted for. The name of the correct configuration file was supplied with the IP configuration (DHCP " file" parameter).

Req 6. The AM **must** provide TFTP servers to host configuration files that correctly configure modems for the services they are entitled to.

DOCSIS defines TFTP file download as the way to configure a modem's operational parameters. Network configuration parameters such as number of attached CPE and CPE IP addresses as well as service parameters such as QoS and bandwidth reservations are set in the configuration file sent to the modem.

DOCSIS defines many configurations and protocols designed to allow a network manager to effectively allocate and manage resources. Primarily, these controls are over bandwidth and traffic priority and are commonly called QoS levels. The service classes that are made available to ISPs by AMs are based on modem configurations that implement QoS levels. The AMs will create DOCSIS service definitions that implement the IP transport classes matching the bandwidth and QoS agreements that have been made with ISPs. This is the subject of Requirement 3, above.

4.3.4 Register with CMTS

After the CM downloads the configuration file it will configure itself according to the parameters received in the file. The modem then will attempt to register with the CMTS it is connected to by sending a copy of its configuration. All of the resource requests must be satisfied for the registration attempt to succeed. If the request fails, the modem will reset and reinitialize its MAC connection.

If resources are not available to permit modems to register, consumers will experience connectivity failures at random times that may be

difficult to diagnose. The AM capacity activation model should be based on dynamic service additions to minimize the possibility that modems will be unable to register. This benefits consumers regardless of their ISP as well as minimizing trouble calls to both AMs and ISPs.

4.3.5 Pass consumer traffic

Following registration, the modem is a fully configured network element. It responds to management requests and is capable of passing traffic from attached CPE.

4.3.6 Modem Software Upgrades

New software will be released for CMs from time-to-time to upgrade features and correct bugs. DOCSIS provides two techniques for determining when a modem will receive a software download.

- If the Software Upgrade Filename parameter (Type = 9) delivered in the configuration file is different from the name of the software image currently loaded, the modem will request a download of the named file.
- A management station sets the MIB variables docsDevSwServer, docsDevSwFilename, and docsDevAdminStatus.

It is in the AM's interest to keep modem software updated to the most recent versions that will work with their CMTSs. The AM will need to be aware of what modems are in service in the access network and provide space on an update software server to keep the loads current.

Processes will need to be established for delivering the upgrades to individual modems and resolving problems for modems that become out-of-date.

4.4 Requirements for Tunneling Through Routed Networks

The Consumer PC is able to pass traffic once DOCSIS connectivity (IP and modem configurations) is established. At this point, the PC must be configured with IP address, default gateway, name servers, etc. This configuration can be obtained from a DHCP server or manually configured into the PC.

Requirement 4 above specifies that traffic destined for different ISPs must be separated until it reaches the ISP's network. This is accomplished by creating an IP tunnel to the ISP Router. Tunnels can be created through this network at Layer 3 using protocols such as L2TP or PPTP[3]. The Consumer uses a client-side application that signals the tunnel server to establish authenticated access from Consumer to ISP. The Dial-up Networking application supplied with Microsoft Windows systems is an example of such an application.

[3] Testing performed in Canada under auspices of the Canadian Cable Telecommunications Association used Cisco Generic Router Encapsulation (GRE), to tunnel through the network.

AOL(2)001865

Tunneling through a routed network requires the host tunnel endpoint to have an IP address in a routing domain of the AM's distribution network as well as an IP address in the ISP's space. If the tunnel server is located inside the AM distribution network, the PC IP address can be private. If the tunnel servers are located outside the distribution network, the PC IP address must be Internet-routable.

The PC will have an IP address assigned to its PC-to-Modem interface. This address must be routable through the AM network to the POI of the ISP chosen by that consumer. The AM assigns this address from either a non-Internet routable space or a public address space.

Tunneling software running on the PC creates a connection to the tunnel service running on the ISP router. All packets delivered by application layers on the PC will be sent over this connection in a point-to-point manner-this is the tunnel. When this connection is created, the tunnel software will acquire an address within the ISP network. Applications running on the PC use this address as their source IP address and deliver packets to the tunnel software for transmission to the tunnel server. There, they are extracted from the tunnel and sent to their destination through the ISP network.

Req 7. The AM **may** allocate non-Internet routable addresses to the consumer PC **if** the ISP POI is inside the AM distribution network. However, **if** the ISP POI is made outside the distribution network and Consumers' tunneled packets leave the AM's distribution system, the Consumer PC **must** be given a routable IP address.

The ISP POI inside the distribution network will be reachable by customers of the ISP. The ISP can either terminate a Layer 3 tunnel at this point and route the Consumer's packet in the usual fashion, or can employ policy-based routing to direct the packet to an appropriate destination.

4.5 Requirements for Bridged Distribution Networks

A Bridged network requires a contiguous Layer 2 addressing domain from Consumer PC to ISP router. It is possible to satisfy Requirement 4 without tunneling by creating appropriate filters in a CM, blocking traffic originating in the same HFC MAC domain, and terminating all traffic in a Policy-based Router. However, more realistically, the ISP routers should employ tunneling techniques described above.

Req 8. The AM **must** provide a connection point for the ISP within the bridged network.

Otherwise this becomes a Routed network and the previous section applies.

4.6 Requirements for Policy-based Router Implementations

Effective traffic separation among Consumers of different ISPs requires that all traffic be delivered from the policy router to the ISP, without short-circuiting within the policy router. The ISPs must take their traffic from these aggregation points, and relay it to the destination.

Req 9. The PBR **must** be the first-hop router beyond the consumer PC if the AM implements Policy-based routing to separate consumer traffic.

The network up to the first-hop router forms a single MAC level domain and consumer traffic can be separated using simple filters. At the PBR, consumer traffic is distinguished either by source IP address or PC MAC address and sent on to the appropriate next hop.

One purpose of using policy routing is to classify traffic early and to quickly hand it off to the appropriate ISP. The AM will need to have sufficient interface ports available at each traffic aggregation point that implements policy routing so that all ISPs have the opportunity to accept their traffic at that point. The multiple interface design allows the AM to direct ISP-bound traffic off their routing infrastructure as early as possible. Alternatively, the AM could permit each ISP to originate a tunnel at the PBR. The tunnel would traverse the AM network to the Internet access point and then on to the ISP network.

5 Requirements for Service Definition and Delivery

There are two important functions that must be realized for any HSD service to be delivered over DOCSIS networks. First, is that service definitions for the available IP transport classes must be translated into specific sets of configuration parameters and coded into modem configuration files and other network elements. The second function is to associate consumers that are serviced by different ISPs with the appropriate configuration elements[4].

Each IP transport class available through the access network is defined in part by a set of parameters encoded in a configuration file. These parameter sets are created and maintained by the AM to correspond to the IP transport classes made available to ISPs. AMs may create one or a small number of offerings defined by a corresponding set of generic files, applicable to any modem. When a new modem comes on line it will be assigned one of these files. Alternatively, the AM will create a set of template files that may be customized for each new modem that comes on line.

5.1 Service Provisioning Flows

The essential elements of the service process flows for HSD are:

- Service request and service activation is a three phase process. The consumer makes initial contact to request service installation. Resources, including CMs or other " soft" resources, are assigned in the Cable Operator, AM, and ISP areas of responsiblity. Finally, activation takes place and the consumer is allowed to access their chosen ISP.
- Trouble shooting takes place and help desk calls are placed when service-affecting issues arise. Responsibility for resolution of these issues is assumed by the agreements reached by the Cable Operator, AM, and ISP
- Service upgrade and/or change procedures are established by the same agreements, but can be treated similar to the processes involved in service request and activation.

Only the service request and activation flows are discussed below.

Service provisioning will be based on a flexible provisioning interface made available by the Cable Operator and AM to the ISPs that will define how to allocate capacity, assign IP addresses, establish administrative entries for billing, logging, etc. It is not the purpose of this document to define these interfaces and process flows, only to note

[4] This document only considers the case of one ISP associated with a given CM. If a consumer decides to change ISP, a provisioning cycle is expected to implement the change. Future extensions to support dynamic selection of multiple SPs will be the subject of separate work.

their importance within the context of the possible options for Equal Access solutions.

A reference model for provisioning is introduced here to capture the essential technical flows in a DOCSIS environment. Cable Operator/AMs may implement this in various ways, depending on their existing business process flows. Agreements will have been made between ISPs, AMs, and Cable Operators that provide means to activate the processes that are described here.

5.1.1 Basic Service Provisioning Model

Figure 8 illustrates the components and relationships of the Service Provisioning model. All of these processes can be automated to a large extent and require Customer Service Representatives (CSRs) and System Administrators (SAs) only for some initial inputs.

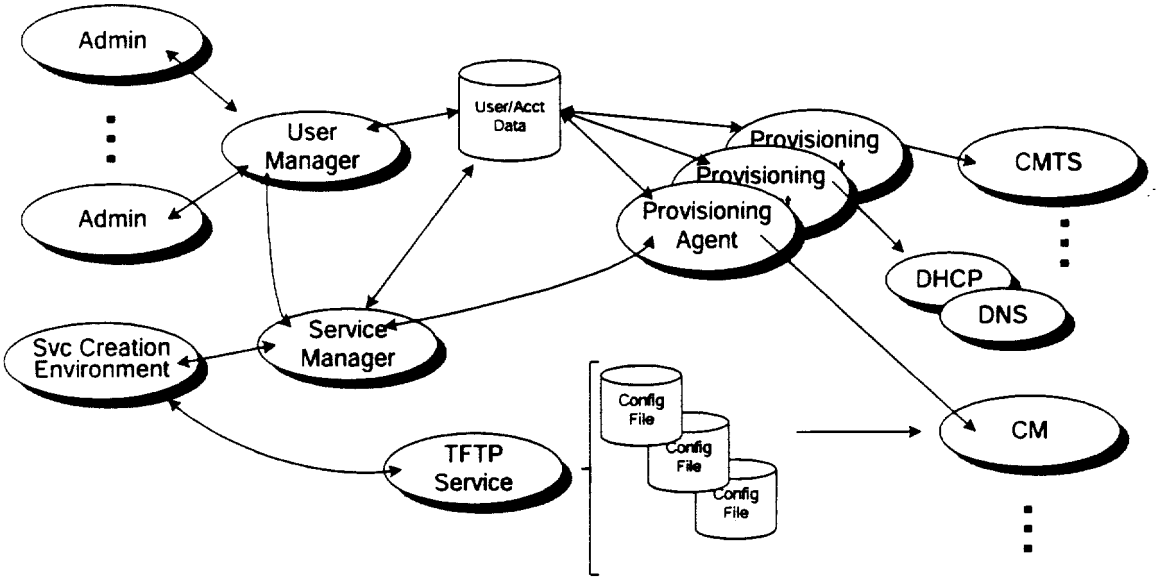

Figure 8 – Elements of modem provisioning services

5.1.1.1 Service Creation Environment

This component translates requirements and specifications for service definitions into configuration files and other parameter settings. DOCSIS requires a CM configuration file that details the data transport services and other network layer capabilities it is allowed. These elements are a component of an overall service offering for consumers.

5.1.1.2 User Manager

The User Manager manages information related to individual consumer accounts. Each consumer is represented by a triplet, (CM MAC, ISP, IP Transport Class). The AM needs to manage this information to understand what modems are allowed to join the network, where to deliver the

traffic originating at the modem, and what the system requirements are for accepting and delivering the traffic.

5.1.1.3 Service Manager

The Service Manager component manages the state of service offerings and binds services to consumers. When a new consumer joins the system or an existing consumer changes the service they receive, the service manager is responsible for mapping the service definitions onto the system elements responsible for delivering service and effecting the required changes.

5.1.1.4 Provisioning Agent

Provisioning Agents have understanding of specific components in a system and translate service definitions into actions on individual devices such as CMTSs or CMs. This is very much a device driver model where there are Provisioning Agents for specific equipment and application gateway types.

5.1.1.5 Admin

The Admin is a person or system (e.g. a Cable Billing System) that is responsible for adding, modifying, and deleting consumer accounts. Some HSD operators have custom systems that perform all customer management and billing functions while others have systems that attempt to use the Cable Operator's in-place systems and processes. However it is implemented, the Admin functions are a necessary starting point for consumers to be given access.

5.1.2 Service Request and Activation

This is the first step in a consumer obtaining HSD service. Many details of process implementation depend on the business models mentioned in the previous section 2. Request and activation consists of 3 phases:

- Service Ordering - A consumer calls for service and requests IP transport and service provider selection. This could be an online process through another service provider or using the flows described below.
- Capacity Activation and Provisioning - Connectivity is established from the consumer premisis and resources are allocated. CMs can be purchased at retail or obtained from one of the providers.
- Service Activation - occurs when the consumer CM is provisioned to permit access to their chosen ISP and the consumer makes an initial login request to the ISP.

These flows are illustrated in Figures 9-11. This set of process flows assumes that the Consumer calls the AM to obtain service and is presented with a menu of service and ISP choices. This view can easily be modified to account for other flows in which the Consumer contacts

the ISP directly (and the ISP must contact the AM for service activation).

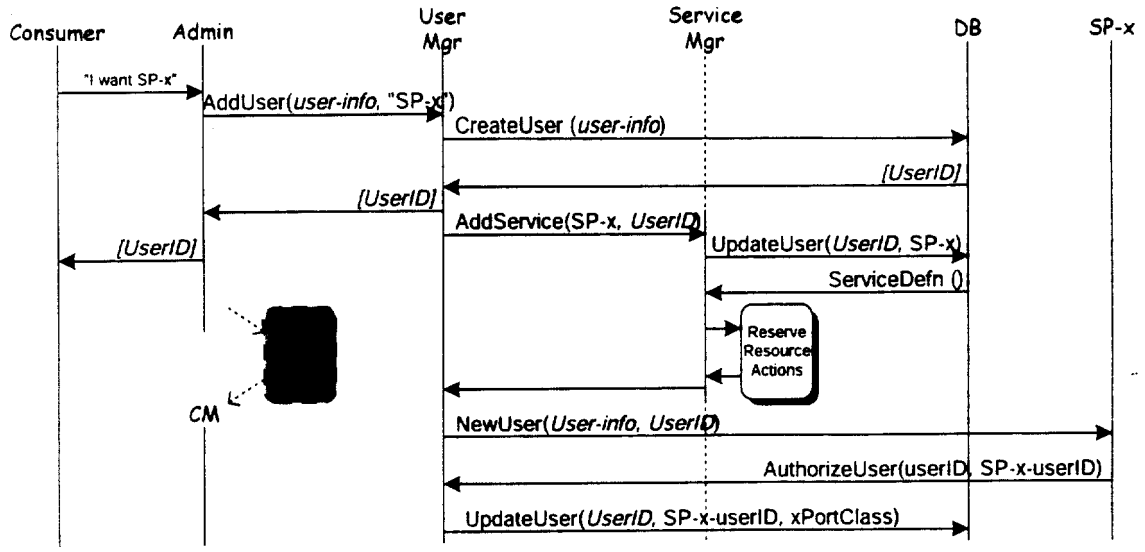

Figure 9 – New user service provisioning flows

5.1.2.1 Service Ordering

Service ordering begins when the Consumer calls the AM to request a service. The Consumer decides on ISP-x and the Admin (a CSR or ACD system) sends a request to the User Manager to add a new user with ISP-x as Service Provider. The User Manager registers the user with the User/Account Database and is given a new UserID in return. The Consumer will later need this UserID to register their CM when service is activated. The Consumer and the Admin continue to determine how the Consumer will obtain and install the CM required for access. The User Manager then requests that the Service Manager add the chosen ISP to the Consumer's profile. The Service Manager updates the Consumer's profile in the User/Account Database and extracts the definition of that service type. The Service Manager can then perform any other local housekeeping necessary to provide that service. Finally, the User Manager can inform the ISP that a new customer has been sent to them.

This completes the service order phase. At this time, the ISP knows a new consumer is coming and has all of the required user information (name, address, etc.), together with the UserID assigned by the AM. The AM has created all of the required database entries and populated them with minimal information, including authorization from the ISP to continue provisioning the user. The Consumer has the assigned UserID and a CM on the way.

5.1.2.2 Capacity Activation and Provisioning

The next phase, capacity activation and provisioning (Figure 10) assigns resources and commits them to a successful installation.

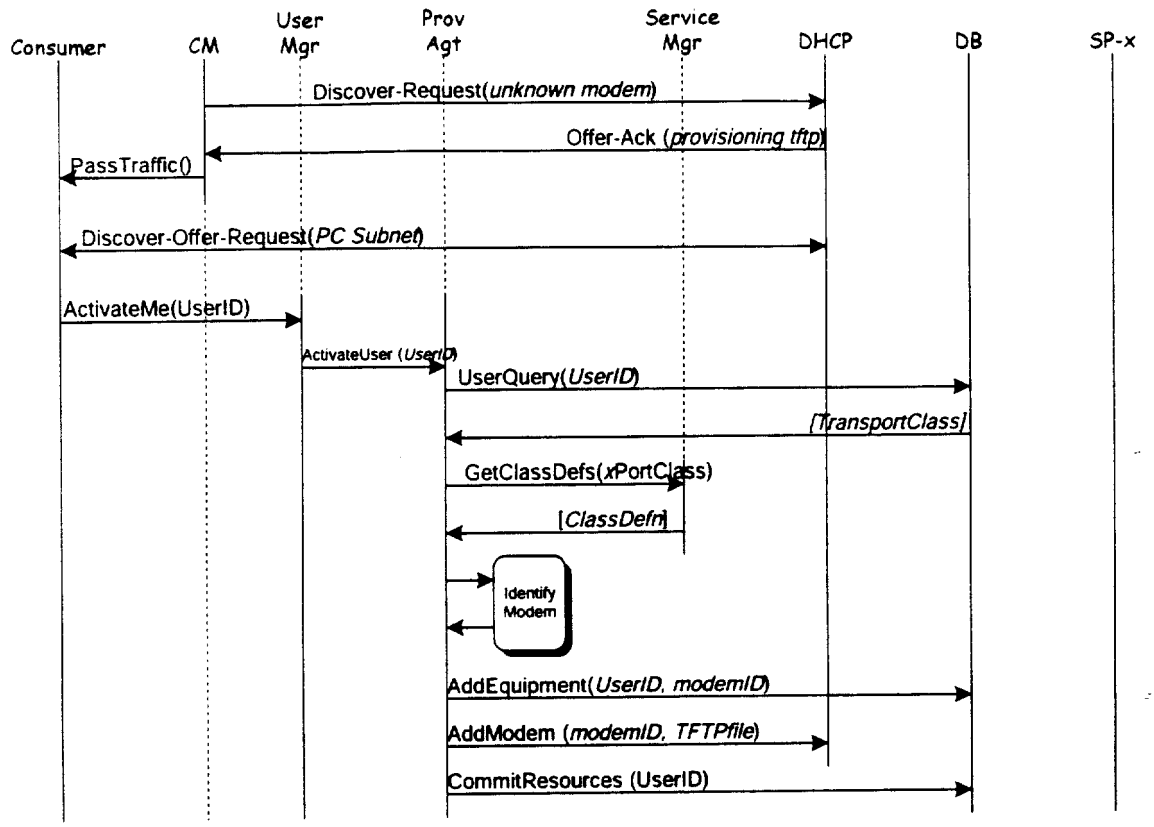

Figure 10 – Capacity activation and provisioning to a consumer

The CM has been installed at the Consumer's residence and connectivity is established. The first step in capacity activation and provisioning occurs when the new CM attempts to acquire an IP address. The modem is unknown at this point so is given an address from a pool that has been set up to allow access to only registration servers. The configuration file delivered to the CM allows access to the provisioning service only. The PC then is allowed to pass traffic only to the DHCP server to obtain an address in the IP transport network and the provisioning server. Using a HTTP/HTML interface the user requests that service be activated for the Consumer indicated by the UserID returned earlier. The Provisioning Agent retrieves the Consumer's records from the User/Account DB then goes to the Service Manager to retrieve the service definitions for the services the Consumer will be provisioned for. The Provisioning Agent performs a process to identify the CM the consumer is using so as to tie together the Consumer, the CM, an appropriate IP address space, and a service-oriented TFTP file.

This completes the capacity activation and provisioning step. All long-lived resources have been committed to the consumer, all of the network services have been provisioned with consumer-specific information, the consumer's modem is known to the AM, and all accounting information has been passed between all parties.