

Figure 11 - Service activation for a consumer

### 5.1.2.3 Service Activation

Service Activation (Figure 11) can take place. The Provisioning Agent has set all the parameters and configurations required for the ISP and IP Transport class the Consumer has chosen. The agent signals a reset to the CM. The CM will restart its IP connectivity process and eventually obtain a configuration file that is specific to the ISP chosen by the Consumer.

The Consumer will then be able to establish connectivity to the chosen ISP and begin the initial dialog with the ISP sign-up process.

This process could be easily modified to the case where the Consumer calls the ISP for service. The ISP could act as the Admin if there was direct access to the OSSs used by the AM, or could relay appropriate information to the AM Admin if no automation was established. The remainder of the flows need not be altered.

In the case where the Consumer first obtains a CM and registers on-line, the Consumer carries on an on-line dialog with a service provisioning agent that implements the Consumer-to-Admin flows.

## 5.2 DOCSIS Configuration Files

Service definitions must be created to properly configure DOCSIS modems. DOCSIS modems have three essential types of configuration parameters.

**Link Layer (LLC) and IP Layer filters**-LLC filters are applied to packets arriving on the CPE-CM interface and are generally intended to limit packets from unwanted protocol types from being sent upstream. IP Layer filters are used to permit or deny passage of packets based on IP header information. They are generally used to limit the kinds of services and destinations that hosts may contact.

**CoS, QoS, and Service Flow definitions**-Bandwidth and packet transmission priorities are allocated to Service Flows that are established between CMTSs and CMs. Service Flows are created for bandwidth and transmission priorities bound into CoS (V1.0) and QoS (V1.1) parameter sets.

**Miscellaneous network parameters**-There are a number of network configuration items that can be varied to create additional services for consumers.

AOL(2)001873

For example, the number of CPE that can send packets through a modem can be limited.

### 5.2.1 Differential Access-Blocking Theorem

If there are multiple, differential destinations and a user is allowed access to only some of those destinations, then access to all others must be explicitly blocked. Unless explicitly blocked, a user simply directs traffic towards the forbidden destinations. If the destinations do not require access validation, then the user obtains services for free from the alternate destination. If access validation is required, and the user is unable to validate, then the possibility of creating denial of service attacks exists.

Figure 12 illustrates a reference model for filter processing. The DOCSIS specification is slightly richer than illustrated (allows for elaborate policy implementation), but the model presented is sufficient for implementing multiple ISP policy.

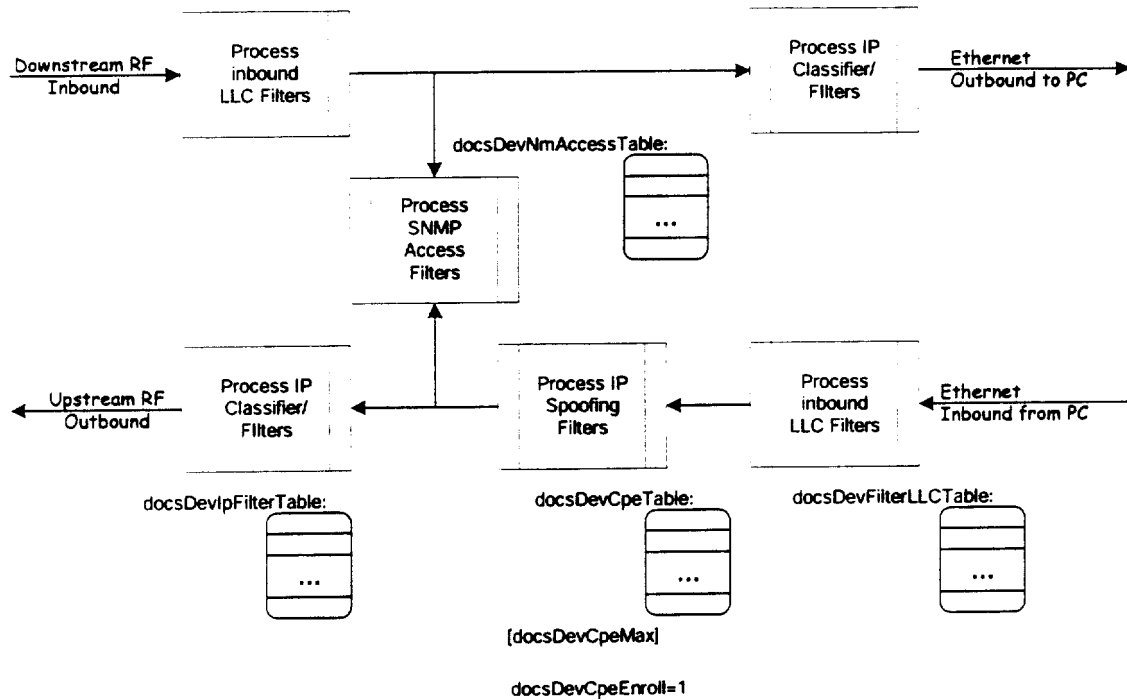


Figure 12 - Model for DOCSIS LLC & IP filter processing.

### 5.2.2 DOCSIS Configuration Requirements

This example of a DOCSIS modem configuration file assumes a routed access network design and two ISPs. It is meant to illustrate the kinds of definitions that would be necessary for a simple Equal Access system.

AOL(2)001874

---

### 5.2.2.1 LLC Filters

LLC filters provide a capability to block traffic based on protocol types that are coded into the MAC-level frames received by CMs (and CMTSSs). Generally these are used to remove traffic from protocols not in use for the IP transport services, such as AppleTalk. There is no need to block access to the local MAC domain, and MAC services as this access is controlled by the CMTS.

### 5.2.2.2 IP Filters

IP filters are used to classify packets passing through the CM and implement policy actions based on the results of the classification process. There are three SNMP MIB tables that are populated with the classification and policy configuration.

IP packet classifiers are described in the docsDevFilterIpTable. This table is an ordered series of rows that contain source, destination, and TOS (IP Type of Service) classifiers, and policy hints for packets that match. The docsDevFilterPolicyTable is used to aggregate policy classes and refer to specific policy action descriptions. The docsDevFilterTosTable is the only currently defined policy action table. This table provides a capability to manipulate the TOS bits in the IP packet header.

The use of IP filters in the CM is intended to separate consumer traffic along the route to their chosen ISP. The Consumer PC may need to acquire an address in the address space of the ISP, but this will be effected through a tunnel if this traffic separation technique is employed. No filters can be created that block legitimate traffic destined for a Consumer's chosen ISP. Filtering rules applied to IP traffic need to meet the following general requirements.

- Req 10.** Essential network services such as DHCP, Time, TFTP, SNMP, and Syslog **must** be available to the modem. DHCP service **must** be available to the Consumer PC so that it can obtain its address in the IP transport space. The AM **must** accept all packets destined for the consumer's ISP interconnection.

### 5.2.2.3 QoS or CoS Definitions

QoS or CoS definitions are created to provide differential service qualities to different modems. Examples of service characteristics that can be manipulated are queue priorities, maximum upstream and downstream bandwidth, and traffic burst limits.

QoS definitions will be created to define the characteristics of Consumer high-speed data traffic and other kinds of services anticipated by the AM/Cable Operator. Different CMTSSs in the same AM access network may have different QoS, created to reflect the demographics, plant quality, or other conditions that exist in the area.

— AOL(2)001875

### 5.2.2.4 Miscellaneous network configuration

A number of configuration parameters that provide increased value to users are available. For example, configuration can limit the number of CPE that can offer and receive traffic through a CM. Some are related to network management and maintenance. For example, it is probably important to not let the CM pass spanning tree information into the Consumer-side.

### 5.2.3 DOCSIS CM Configuration File Example

The configuration is designed to limit users to a single PC that is allowed to receive 1Mb/s downstream and send 512Kb/s upstream. The PC is allowed to create a tunnel to a ISP tunnel server within the AM network. Each needed configuration parameter is expressed as its Tag-Length-Value (TLV) would be written in the binary file sent to the CM at reset.

| Tag   | Length | Value   |
|---|--------|---|
| <i>First some simple access and flow controls</i>   |        |   |
| TLV_NWACCESS  | 1      | On (1)  |
| TLV_MIBOBJ  |        | docsDevStpControl= noStFilterBpdu(2)                    |
| TLV_MAXCPE  | 1      | 1   |
| <i>A set of IP Filters to direct CPE traffic to the ISP of their choice and permit access to essential network services. Discard all packets not matching a filter.</i> |        |   |
| TLV_MIBOBJ  | N      | docsDevFilterIpDefault=discard(1)                       |
| <i>Filter that allows through all packets to the ISP router. Put this first as it will be the most often matched rule.</i>  |        |   |
| TLV_MIBOBJ  |        | <b>docsDevFilterIpIndex.10=10</b>                       |
| TLV_MIBOBJ  | N      | docsDevFilterIpStatus.10=active(1)                      |
| TLV_MIBOBJ  | N      | docsDevFilterIpControl.10=accept(2)                     |
| TLV_MIBOBJ  |        | docsDevFilterIpIfIndex.10=ether                         |
| TLV_MIBOBJ  |        | docsDevFilterIpDirection.10=both(3)                     |
| TLV_MIBOBJ  |        | docsDevFilterIpBroadcast.10=false(2)                    |
| TLV_MIBOBJ  |        | docsDevFilterIpSaddr.10=0 (any)                         |
| TLV_MIBOBJ  |        | docsDevFilterIpSmask.10=0                               |
| TLV_MIBOBJ  |        | docsDevFilterIpDaddr.10= <i>service provider router</i> |
| TLV_MIBOBJ  |        | docsDevFilterIpDmask.10=0                               |
| TLV_MIBOBJ  |        | docsDevFilterIpProtocol.10=any                          |
| TLV_MIBOBJ  |        | docsDevFilterIpSourcePortLow.10=0                       |

AOL(2)001876

|  |   |   |
|--|---|---|
| TLV_MIBOBJ   |   | docsDevFilterIpSourcePortHigh.10=65535      |
| TLV_MIBOBJ   |   | docsDevFilterIpDestPortLow.10=0             |
| TLV_MIBOBJ   |   | docsDevFilterIpDestPortHigh.10=65535        |
| <i>A Filter that allows access to the DHCP Server, by the Consumer PC.</i>                       |   |   |
| TLV_MIBOBJ   | N | docsDevFilterIpStatus.20=active(1)          |
| TLV_MIBOBJ   | N | docsDevFilterIpControl.20=accept(2)         |
| TLV_MIBOBJ   |   | docsDevFilterIpIfIndex.20=ether             |
| TLV_MIBOBJ   |   | docsDevFilterIpDirection.20=inbound(1)      |
| TLV_MIBOBJ   |   | docsDevFilterIpBroadcast.20=true(1)         |
| TLV_MIBOBJ   |   | docsDevFilterIpSaddr.20=0 (any)             |
| TLV_MIBOBJ   |   | docsDevFilterIpSmask.20=0                   |
| TLV_MIBOBJ   |   | docsDevFilterIpDaddr.20= <i>DHCP Server</i> |
| TLV_MIBOBJ   |   | docsDevFilterIpDmask.20=255.255.255.255     |
| TLV_MIBOBJ   |   | docsDevFilterIpProtocol.20=udp              |
| TLV_MIBOBJ   |   | docsDevFilterIpSourcePortLow.20=68          |
| TLV_MIBOBJ   |   | docsDevFilterIpSourcePortHigh.20=68         |
| TLV_MIBOBJ   |   | docsDevFilterIpDestPortLow.20=67            |
| TLV_MIBOBJ   |   | docsDevFilterIpDestPortHigh.20=67           |
| <i>We can use simple V1.0 CoS since there is a single data rate and only 1 service available</i> |   |   |
| TLV_V1COS  |   |   |
| COS_CLASSID  | 1 | 1   |
| COS_MAXDSRATE  | 4 | 1000000                                     |
| COS_MAXUSRATE  | 4 | 512000                                      |
| COS_USCHANPRI  | 1 | 4   |
| COS_MAXUSBURST   | 2 | 254   |
| COS_BPENABLE   | 1 | Enable (1)                                  |
|  |   |   |

AOL(2)001877

## 6 Example Implementations

In this section we present several reference designs to illustrate network connectivity, IP address allocation schemes, and LLC and IP filter requirements. Manufacturers and equipment types are illustrative only. Specific components are included because they are representative of the capabilities and availability needed for the design. There may be many equivalent network elements and equipment configurations that would be applicable in each instance.

### 6.1 Small Cable Operator

Small Cable Operators will typically have fewer than 50,000 Homes passed and will site their entire HSD offering in a single headend distribution hub. Figure 13 illustrates the system design for such an operator. Two moderately loaded CMTS units could service the entire area. The AM distribution network would consist of a switched Ethernet that interconnects all of the management systems and ISP systems. The system elements indicated in the figure are chosen to illustrate typical system sizes and through-put requirements for such a system.

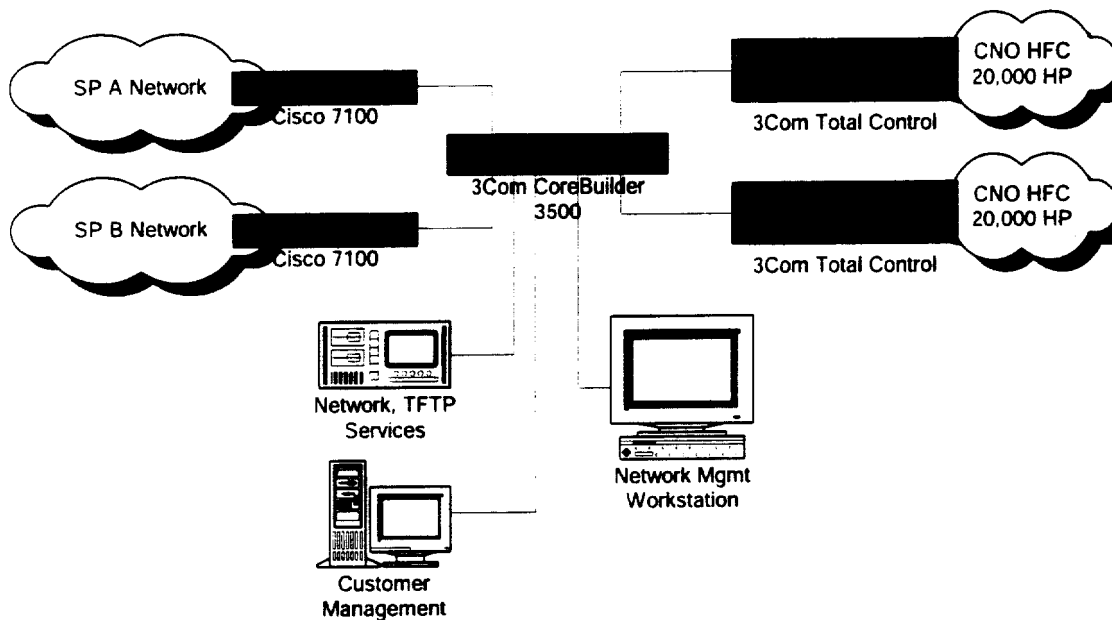
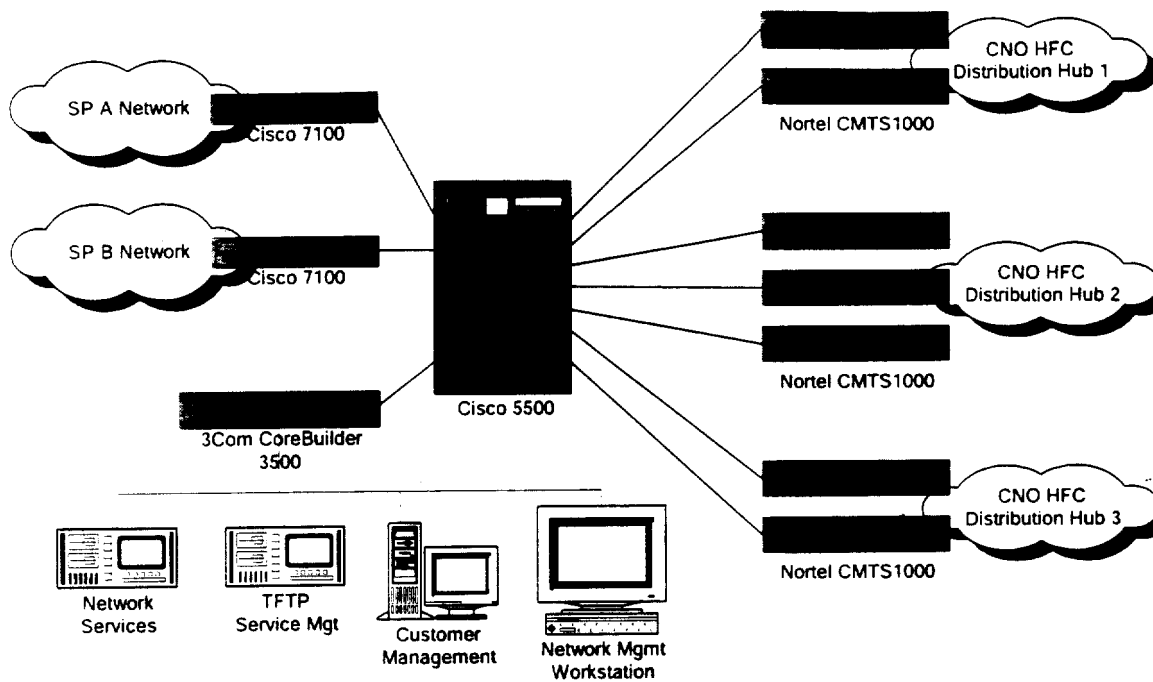


Figure 13 - Small Cable Operator system design

### 6.2 Bridged Network Reference Model Design

A Bridged network can be constructed using Fiber Distributed Data Interface (FDDI), ATM, or Ethernet Switches. Figure 14 illustrates a possible architecture.

AOL(2)001878



**Figure 14 - Bridged System Design**

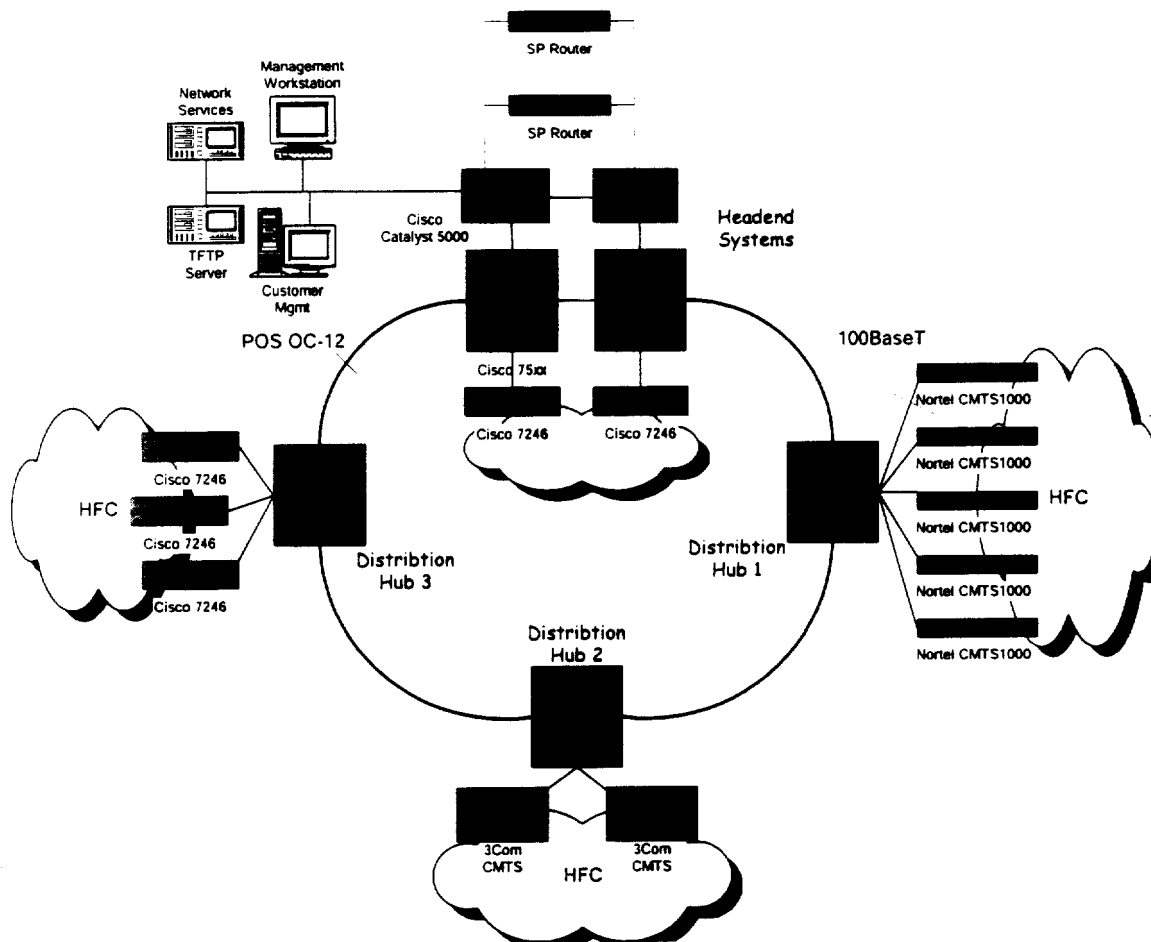
The bridged network design is good for moderate sized cable plants in which point-to-point links can be established to the distribution hubs not co-located with the headend systems. The remote hubs can be reached using any of the switched technologies, sometimes requiring extenders to lengthen the reach of the switching network element.

### **6.3 Routed Network Reference Model Design**

Routed distribution network designs are effective when the area to be covered is larger than a single metropolitan area, such as a moderate sized city and its surrounding suburbs. The Cable Operator plant might be 30-150 miles in diameter. This type of design provides for redundant paths to the distribution hubs and highly available headend interconnects.

Figure 15 illustrates a routed network reference model.

AOL(2)001879



**Figure 15 - Design of a Routed distribution network system**

The network illustrated in 15 is a simple single ring design. In practice there may be many subtended rings or other MAN connectivity. This type of design would be typical in a large cable plant with rich fiber interconnectivity. The Cable Operator would have multiple diverse routes to each distribution hub that provide capability to create redundant, protected service.

The distribution network could employ a Sonet infrastructure to carry any number of network types or a Packet-over-Sonet network could be created directly in the fiber paths. This type of distribution network has many growth paths for capacity and service delivery. Given the multiple router hop nature of the distribution network, IP-level tunneling would be the most flexible Equal Access technique.

AOL(2)001880



---

## 7 Management and Operations Requirements

### 7.1 SLA Considerations

The AM/CNO and the ISPs will create Service Level Agreements (SLA) to specify what they will provide each other. Generally, an SLA consists of specifications for:

- Type of service.
- Expected performance described by a metric and its value.
- A measuring methodology for the metric.

The SLA for HSD services should be expressed in terms of the service that an individual modem will receive. The AM and Cable Operator construct plant and network capacities to satisfy a projected service take rate and churn. The amount of bandwidth delivered to a CMTS, the number of CMTSs, and the number of users expected determines the configuration of each CMTS.

- Common SLA metrics include:
  - Network availability - the percentage of time that the network is available.
  - Utilization - Actual traffic delivered divided by the Contracted capacity.
  - Packet Loss Ratio - the number of packets lost over the number of packets offered.
  - Latency - one-way delay measured at agreed upon ends of a connection.
  - MeanTime to Repair - how long it takes from problem reporting to final resolution.
  - Mean Time to Install - how long it takes to install a service following a request.

### 7.2 ISP visibility into AM management systems

Under certain circumstances it might be necessary for ISPs to have visibility into AM network management systems. Appropriate agreements will need to be created between ISPs and AM to cover (at least) the following needs:

- Troubleshooting and resolution needs - Consumers will experience delays and outages due to faults in the Cable Operator HFC or AM distribution networks. In order to minimize troubleshooting costs to the AM it is reasonable to permit ISPs to read network status from their own network operations centers. Adequate access controls and filtering should be put in place and use of standard network management tools would greatly assist problem troubleshooting and resolution tasks.

AOL(2)001881

- 
- SLA monitoring requirements - Visibility into each other's networks would facilitate management and monitoring of counters and variables that form the basis for service level agreements.

AOL(2)001882

---

## 8 Scalability and Performance Considerations

There are three main areas that need to be addressed in order for multiple service provider systems to grow and perform consistently: traffic, total customer base, and total number of ISPs. Traffic and customer base are not unique effects of having multiple ISPs. The growing interest in HSD services delivered over cable systems drive the customer base up regardless of the number of ISPs that are available at a given location. The number of ISPs may cause the growth in customers to occur sooner.

### 8.1 Traffic

The design and operation of the shared DOCSIS access network must be upgraded on a continuous basis as the traffic grows based on the IP transport classes defined by the AM. Clearly access network traffic is dependent on the number of customers to be serviced.

Traffic modeling and capacity planning will ensure that average and peak usage of the network will be maintained within the performance ranges specified by the IP transport classes offered by the AM.

Traffic through the access network is constant for a given number of consumers and IP traffic class, without regard to the number of ISPs or the aggregation points at which traffic is separated.

The AM should seek to deliver all ISP-bound traffic to ISPs within the access network. When the AM has structured the Equal Access architecture to deliver ISP traffic through a border router to the Internet, the AM will bear the cost of the Internet access bandwidth.

### 8.2 Total Number of Customers

Certainly, as the number of consumers that are serviced by the system grow, service delivery components (in addition to the traffic capacity) must be sized and grown in proportion. Per-consumer services supplied by the AM will grow linearly with the number of CMs installed. The DOCSIS-required services, DHCP, RFC868 Time, TFTP, and Syslog are all components that must grow with the user base.

Mutual exchange of information will minimize Consumer inconvenience due to lack of adequate resources.

- Req 11.** The AM **must** provide periodic traffic reports for each IP transport class to each of the ISPs that use that class for service delivery. The ISPs **must** provide estimates of customer growth to the AM for purposes of capacity planning within each of the IP transport classes.

The total number of consumers drives the traffic model and network services capacities, not the number of ISPs. It is expected that availability of multiple ISPs may bring consumers into the system that would not ordinarily have bought HSD services. The Cable Operator and AM must have the required traffic monitoring and business processes to maintain the offered IP transport classes within established parameters.

AOL(2)001883

---

### **8.3 Total Number of ISPs**

The total number of ISPs that are available at a particular system increases the number of interconnection points that must be made available to the AM distribution network. The discussion in Section 3 identifies two kinds of interconnections necessary to carry traffic from access networks to ISP networks: tunnel endpoints and interface ports on network elements. The number of interconnections grows as the interconnection points are driven deeper into the network.

AOL(2)001884

---

## 9 Open Issues

### 9.1 Multicast

Multicast is of particular interest because it is a distinguishing feature of shared-access broadband networks. Efficiently used it can be a powerful technique for multiple-participant sessions. However, multicast only makes sense when there are multiple listeners on a broadcast-capable network media. Several possibilities exist for efficient multicast delivery.

Solutions that are based on leased multicast "channel" capacity (rent-a-channel) to provide all multicast and broadcast streams for all subscribers of a particular ISP would be difficult to implement and suffer from the same problems that providing RF overlays as a traffic separation technique have - only on a dynamic scale.

More promising is to use the protocols and facilities that are in place to service multicast. Multicast group membership would be managed by the ISP point-of-presence, rather than as an arrangement between client and multicast router. This relies on traffic being encrypted on the shared access portion of the network and the ability of the point-of-presence system to register users with the multicast router in a proxy fashion.

If a strict DOCSIS solution is employed, the AM must provide multicast Service Flow Identifiers (SFIDs) on an equitable basis to ISPs. The AM can specify limits on their use based on non-discriminatory basis to all ISPs.

### 9.2 Multiple Service Providers to a Single Consumer

In an Equal Access environment, it is conceivable that a consumer would select multiple ISPs because each might have particular unique services attractive to the consumer. Some consumers might select multiple providers because of past associations that are easy to maintain in dial-based environments. The requirements outlined in previous Sections do not specifically address multiple providers to a single consumer, although care has been taken to design requirements that do not bar this possibility.

The general outline of multiple providers to a single consumer would be that configurations are additive. A consumer expecting service from ISP A as well as ISP B would have a configuration that was the union of the two configurations. The consumer would be responsible for determining which ISP (A or B) was to receive traffic during any given session.

AOL(2)001885

---

## 10 References

- [DevMIB] St. Johns, M., ed., Cable Device Management Information Base for DOCSIS compliant Cable Modems and Cable Modem Termination Systems, draft-ietf-ipcdn-cable-device-mib-07.txt, Feb 1999.
- [DocsisV1.0] Data-Over-Cable Service Interface Specifications, Radio Frequency Interface Specification, Cable Television Laboratories, ISP-RFI-I04-980724, July 1998
- [DocsisV1.1] Data-Over-Cable Service Interface Specifications, Radio Frequency Interface Specification, Cable Television Laboratories, ISP-RFIV1.1-I01-990311, March 1999
- [RFC868] Postel, J., Harrenstien, K., Time Protocol, IETF RFC-868, May 1983
- [RFC1661] Simpson, W., Ed., The Point-to-Point Protocol (PPP), IETF RFC-1661, July 1994
- [RFC2328] Moy, J., OSPF Version 2, April 1998
- [RFC2453] Malkin, G., RIP Version 2, November 1998
- [RFC2516] Mamakos, L., Lidl, K., Evarts, J., Carrel, D., Simone, D., Wheeler R.. Method for Transmitting PPP Over Ethernet (PPPoE), February 1999
- [RFC2661] Townsley, W., Valencia, A., Rubens, A., Pall, G., Zorn, G., Palter, B., Layer Two Tunneling Protocol "L2TP". August 1999
- [RFC2637] Hamzeh, K., Pall, G., Verthein, W., Taarud, J., Little, W., Zorn, G., Point-to-Point Tunneling Protocol, July 1999
- [RFMIB] St. Johns, M, ed., Radio Frequency (RF) Interface Management Information Base for MCNS/DOCSIS compliant RF interfaces, draft-ietf-ipcdn-rf-interface-mib-07.txt, February 1999.

AOL(2)001886

## Appendix A. The Routing Fish

The routing fish is a phenomena created by the next-hop nature of Internet routing protocols and the decentralized control model presented by IP. The routing fish occurs when multiple independent consumers attempt to reach a common destination through a common router, but desire their traffic to be delivered through separate providers. This is illustrated in Figure 16.

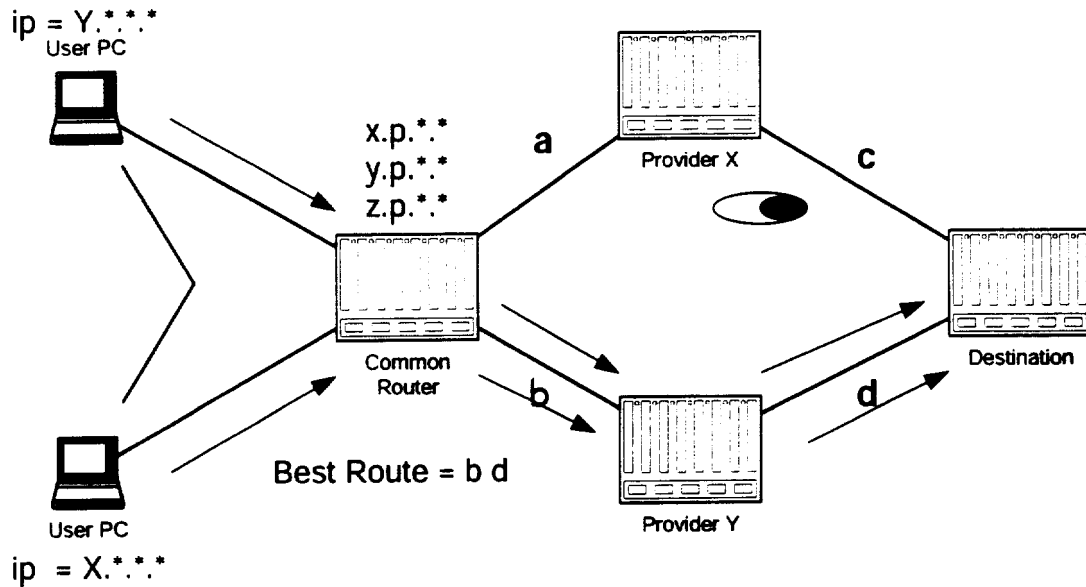


Figure 16 - Routing fish

The best path from the common router to the destination is along links (b,d). The common router will always select this path (under normal steady-state conditions), which is based on destination address, irrespective of source address. If packets were forced (Policy routed) to the proper service provider from the common router, i.e. route (a,c) was picked for user X.p.p.p., the routing fish is still problematic. In this case, the packets directed to X.p.p.p. from the destination (return acknowledgements or replies) would still traverse the more efficient (d,b) link.

AOL(2)001887

## Appendix B. List of Acronyms

| Acronym | Long Form                                       | Definition   |
|---------|---|--|
| ACD     | Automatic Call Distribution (system)            | One of those annoying voice answering systems that ask you to choose a menu item at each point in the decision tree that leads to your ultimate goal with the call.  |
| AM      | Access Manager                                  | The party that implements and is responsible for IP networking over a Cable Network Operator's physical plant.   |
| CM      | Cable Modem                                     | Component of CATV HSD system that is downstream at a customer's premises. It connects to the HFC plant on one side and the customer's host PC on the other.  |
| CMTS    | CM Termination System                           | Component of CATV HSD system that is upstream at a cable distribution hub or headend. It connects to the data distribution network on one side and the HFC plant on the other side.  |
| CNO     | Cable Network Operator                          | The party that owns and operates the physical CATV distribution plant in a particular cable franchise area.  |
| CPE     | Customer Premises Equipment                     | Equipment that a customer has plugged into a CM.. Generally this would be a PC, but could include any network implementation that the consumer has plugged into the CM.  |
| CSR     | Customer Service Representative                 | An agent that consumers call to order goods and services from providers. CSRs are usually able to take orders for new services or upgrades, adjust bills, direct the caller to a help desk when there are problems, and schedule service callsh. |
| DOCSIS  | Data Over Cable Service Interface Specification | Set of physical, data-link, operations, and management specifications for delivering HSD over cable TV distribution plants.  |
| HFC     | Hybrid Fiber Coax                               | Cable distribution plant implementation that uses fiber optic cable to deliver signals to nodes that supply approximately 500 Homes passed   |
| HSD     | High-Speed Data                                 | CM or DSL -based Internet connectivity.  |
| IP      | Internet Protocol                               | Suite of communications protocols sponsored by IETF  |
| L2TP    | Layer 2   |  |

AOL(2)001888



|       |                                       |   |
|-------|---------------------------------------|---|
|       | Tunneling Protocol                    |   |
| LLC   | Link Layer Control                    | Layer 2 in the ISO reference model. This is the layer at which frames are created and impressed on the physical layer of a data network.  |
| MSO   | Multiple System Operator              | Cable Operator that operates more than a single system.   |
| OSS   | Operations Support System             | A set of computer-based processes and programs that manage distribution equipment and support back office business flows used by a cable operator.  |
| PBR   | Policy-Based Router                   | A router that implements routing decisions based on attributes and fields of packets, other than destination address. Policy-Based Routing does not use routing tables based on common routing protocols to form next-hop decisions for packets. For example, a policy router could forward packets based on type of service or source address. |
| POI   | Point-of-Interconnection              | This is the physical interface port at which a connection is made from an AM's network to the ISP's network.  |
| PPTP  | Point-to-Point Tunneling Protocol     |   |
| PPPoE | Point-to-Point Protocol over Ethernet |   |
| RF    | Radio Frequency                       | The electromagnetic band used by cable operators to deliver signals through their cable distribution plant.   |
| ISP   | ISP                                   | The party that provides internetworking services to consumers.  |
| TLV   | Tag-Length-Value                      | A coding technique for data values in which the transmitted value is represented by a triple of: Tag - a 1 byte number that tells what the datatype of the value is; Length - number of bytes in the data value; Value - the actual bytes of the data value.  |
| VPN   | Virtual Private                       | Network implementation technique in which the services and protocols of a network technology are embedded in another network's protocol.  |

AOL(2)001889

---

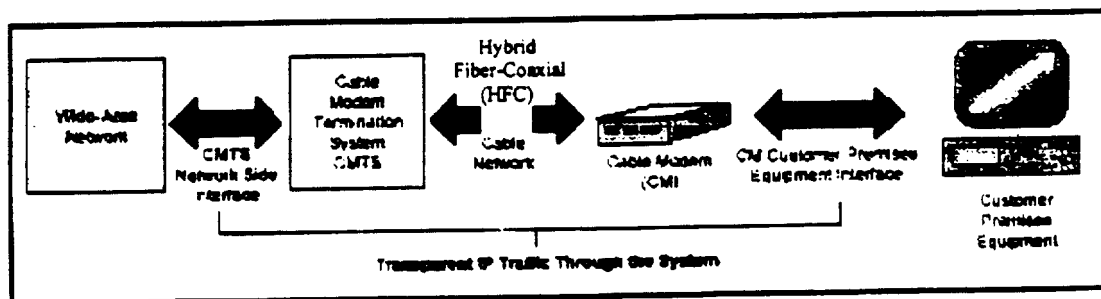
|  |         |  |
|--|---------|--|
|  | Network | This is generally an end-to-end design that supplies certain connectivity constraints and security and privacy features. |
|--|---------|--|

AOL(2)001890

## DECLARATION OF SUK S. SOO

I, Suk S. Soo, hereby declare as follows:

1. My name is Suk S. Soo and I am Vice President - Special Projects for AOL Technologies. I am responsible for the technical assessment of various broadband platforms as they relate to the business interests of America Online, Inc. ("AOL").
2. I joined AOL in February, 1998. Prior to that time, I was Vice President of ANS Communications, a wholly-owned subsidiary of AOL until it was sold to WorldCom in 1998, and I oversaw the build-out of the ANS portion of AOLnet. Prior to joining ANS in 1993, I had a 30-year career at IBM Research Division, holding various senior technical and management posts, including being appointed a member of IBM's Corporate Technical Committee. During my tenure at IBM, I authored in 1986 the successful bid by IBM, MCI, and Merit for building the NSFnet, the precursor to the modern Internet.
3. The network and systems infrastructure deployed by the cable industry for broadband IP services over the Hybrid Fiber Coax access plant is based on open, interoperable standards. Under the sponsorship of Cable Labs, the cable industry technical organization, a "de-facto" set of standards has been issued. Collectively known as the *Data-Over-Cable Service Interface Specification (DOCSIS)*, these standards can be referenced at <http://www.cablemodem.com>.



**Figure 1-1. Transparent IP Traffic Through the Data-Over-Cable System**

A simplified representation of the Data-Over-Cable infrastructure is shown in Figure 1-1, as abstracted from the DOCSIS documentation. The transmission path over the cable system is realized at the headend by a Cable Modem Termination System (CMTS), and at each customer location by a Cable Modem (CM). At the headend (or hub), the interface to the data-over-cable system is called the Cable Modem Termination System - Network-Side Interface (CMTS-NSI) and is specified in

[DOCSIS SP-CMTS-NSII01-960702]. The interface of the CMTS to the HFC network is specified by [DOCSIS SP-RFI-I04-980724]. At the customer location, the interface is called the cable-modem-to-customer-premises-equipment interface (CMCI) and is specified in [DOCSIS SP-CMCI-I02-980317]. The intent is for MSOs to transparently transfer IP traffic among these interfaces.

4. There are many possible points where multiple Service Providers can interface to the cable system on an open access basis. We will treat herewith the interface at the CMTS-NSI, as a demonstration of how this open access can be implemented.

- **HFC configuration**

From the CM to the CMTS there will be no change in implementation between a system built for a single Service Provider and a system that is open to multiple Service Provider access since the HFC medium is shared by all. More specifically, any capacity issues that might arise will be a function of the total number of subscribers of the data-service, and not a function of the number of Service Providers.

- **Data link and Physical access**

There are several standard communications interfaces specified at the CMTS-NSI, *e.g.*, ATM over DS3 or Ethernet over 100BASE-T. Each Service Provider that desires access over the cable plant to the end-user must interface through these standard mechanisms at the cable head-end where the CMTS is located. The specific choice of the mechanism will be a function of the selection made by the CMTS owner. No change to the existing physical configuration will be required. The number of Service Providers that can be accommodated is limited only by the number of ports made available at the CMTS-NSI, which in theory is unlimited, and in practice probably more than the number of Service Providers that will choose to obtain access.

Once such a link is established, any end-user has a physical and logical path available to access the Service Provider. In addition, however, proper addressing routing configuration (a software task) must be established for multiple Service Providers so that each customer will be able to select the Service Provider of choice.

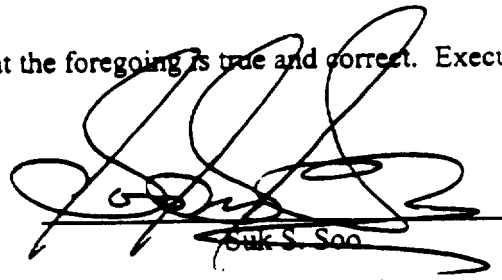
- **Addressing Routing Configuration.**

The IP addressing and routing must be configured to direct the traffic to the appropriate gateway router and backbone network of the designated Service Provider of the customer, through the data link at the CMTS-NSI interface. There are many ways to achieve the required addressing and routing configuration to support multiple Service Providers. We illustrate, by example, one approach.

| <b><u>IP addressing and routing configuration</u></b><br><b><u>(example of a solution)</u></b>    |  |
|---|--|
| <b>Unitary Service Provider</b>   | <b>Multiple Service Providers</b>  |
| <b>Initial setup</b> (static, at provisioning, or dynamic, at session log-in)                     |  |
| 1) CM establishes connectivity and registers with CMTS.   | 1) CM establishes connectivity and registers with CMTS.  |
| 2) PC (TCP/IP stack) broadcasts DHCP request, including source identifier (e.g., PC MAC address). | 2) PC (TCP/IP stack) broadcasts DHCP request, including source identifier (e.g., PC MAC address).  |
| 3) CMTS receives requests, and relays it to the DHCP server.                                      | 3) CMTS receives requests, and relays it to the DHCP server.   |
| 4) DHCP server looks up available IP addresses.   | 4) DHCP server looks up available IP addresses, <i>per each Service Provider configuration as indicated by source identifier.</i>              |
| 5) DHCP server responds, including assigned IP address for PC.                                    | 5) DHCP server responds, including assigned IP address for PC, <i>and gateway router address corresponding to customer's Service Provider.</i> |
| 6) CMTS relays response to PC.  | 6) CMTS relays response to PC, <i>but first stores gateway router address indexed by source identifier.</i>                                    |
| 5) PC configures its TCP/IP stack with IP address from Service Provider block.                    | 5) PC configures its TCP/IP stack with IP address from <i>customer's Service Provider</i> block.   |
| <b>Traffic flow</b> (customer activity)   |  |
| 1) PC (TCP/IP stack) generates traffic through CM to CMTS.  | 1) PC (TCP/IP stack) generates traffic through CM to CMTS.   |
| 2) CMTS routes traffic to the next hop gateway router.  | 2) CMTS routes traffic to the <i>appropriate next hop gateway router based on table lookup from source identifier.</i>                         |
| 3) Return traffic comes to gateway router (recognized by source IP address), through CMTS to CM.  | 3) Return traffic comes to <i>appropriate Service Provider gateway router (recognized by source IP address)</i> , through CMTS to CM.          |

The required changes to support multiple Service Providers are straightforward: configuration of the DHCP server to store the table of IP address blocks by Service Provider and by source identifier, and the configuration of the CMTS to store the table of next-hop gateway router addresses by source identifier. While there will be other solutions that may be better tailored to specific implementation details, it is clear that there are technical solutions for the proper IP addressing and routing configuration to support customer choice among multiple Service Providers.

5. I declare under penalty of perjury that the foregoing is true and correct. Executed on this 29<sup>th</sup> day of October, 1998.



Guk S. So

**AMENDMENT TO  
AGREEMENT**

**FIRST AMENDMENT TO  
INTERACTIVE SERVICES  
AGREEMENT**

**AOL TV CONTENT  
AGREEMENT**



**MARKETING TEST  
AGREEMENT**