On Management of CATV Full Service Networks: A European Perspective

Saleem N. Bhatti and Graham Knight
University College London

Abstract

The CATV network operators hope to offer digital services and evolve their networks to full service networks. There are many hurdles for them at the moment in the transition to a digital network and digital service offering from the current analog-based technology. Key to the success of the transition will be a well-integrated and capable management system to allow CATV operators and service providers to control the network as well as the services they will offer. The CATV operators need to agree on a common data communication infrastructure and plan how their new digital services will be offered to subscribers without disrupting the current customer base of analog service users. The choice of network technology and data communication protocols will have a strong influence on the network management technology chosen. A vital element for the provision of a common open communication architecture as well as for the purposes of network management is that IP is used. The adoption of existing standards is vital in order to establish a fast route to open network management for CATV networks. It is possible that CATV operators and service providers will have to integrate existing SNMP management systems and TMN/OSI management, with newer integrated service management systems based on TINA and implemented on a CORBA platform. There is a strong need to address security issues before any of these technologies can be deployed for service. There is currently investment (deployed systems and research) which uses each of the technologies mentioned, so these technologies will need to coexist. This article highlights the differences between the North American and European network architectures, and outlines the European network and network management scenario. This is based on the authors' involvement in a Pan-European CATV project, Integrated Broadband Communication over Broadcast Networks — IBCoBN.

The cable TV (CATV) providers' original market was that of home entertainment. CATV operators designed and implemented their networks so that they could broadcast analog TV signals on a terrestrial network. Many of the networks in both North America and Europe maintain their original physical architecture, consisting of coaxial cable (coax) with passive repeaters, fed from local distribution points (street cabinets), as shown in Fig. 1. The cable runs along the street with coax feeds to the home. CATV companies now see their networks becoming full service networks (FSNs) and offering data services. The North American and European operators realize they can offer a much broader service portfolio than they currently have, including traditional telephony as well as *broadband digital delivery* of services.

Indeed, the CATV operators have the raw bandwidth in the ground to offer broadband residential data services, and could compete in a very cost-effective way with suppliers of such services as narrowband integrated services digital network (ISDN) (basic rate and primary rate), leased lines, digital subscriber loop (xDSL), and traditional dial-up services such as public switched telephone network (PSTN). However, in many cases the legacy installation and services are holding back the deployment of high-speed data services. The analog networks of the CATV providers must be adapted from a fairly simple one-way analog broadcast model to a more complex system which supports digital information exchange. Additionally, the CATV operators see themselves eventually offering their entertainment services over digital channels rather than the current analog channels, so they are keen to establish experience and knowledge about how they might make the transition from their current technology to digital transmission and delivery systems. Their goals do not just include simply offering their current services via a digital system, but also exploiting the new service possibilities offered by the transition to a digital system. This includes the provision of data services such as those offered via the Internet. The provision of such data services is where the European and North American approaches differ.

This article is based on work conducted by the authors within the Integrated Broadband Communication over Broadcast Networks (IBCoBN) project, a European-Community-funded project involving CATV operators from all over Europe. This article highlights the differences between the European and North American networks, and presents the issues from the particular viewpoint of network management for CATV FSN networks.

We start by considering the current and (near-term) future technology for management of network components and networks in the next section. We then look at the provisioning of a common communications infrastructure for the CATV networks. This is followed by a look at issues concerning integrated service management. We conclude with a short summary.

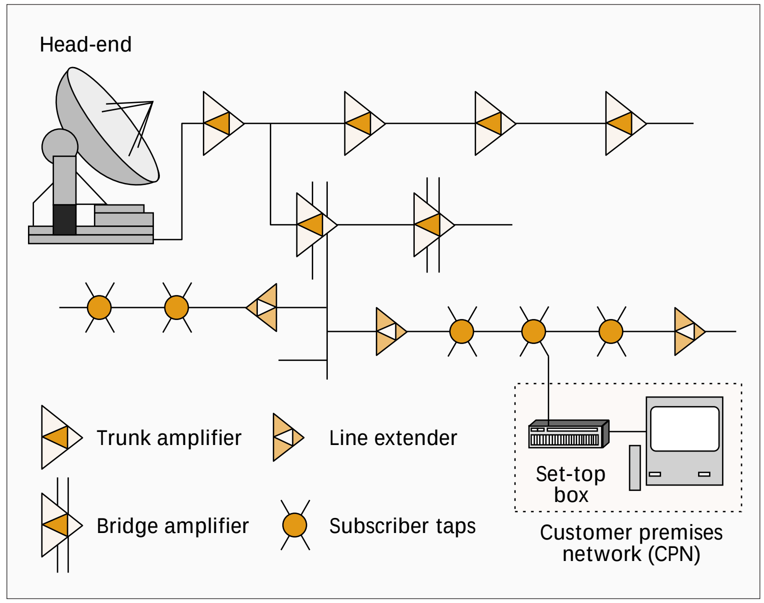


Figure 1. *Current mature coax networks.*

Management of Networks and Network Elements

Standardization at the Physical Layers

CATV networks around the world vary considerably in their use of network technology. For digital transmission there are currently many modulation and coding schemes in use. One of the reasons for the differences in CATV networks around the world is the lack of standardization in the CATV community, especially compared with the telecom sector. The issue of standardization is currently being addressed by such bodies as:

- IEEE 802.14 Working Group (WG) and ATM Forum Residential Broadband WG (North America based, but with worldwide participation)[1]
- European Telecommunications Standards Institute (ETSI) and CENELEC (Comité Européen de Normalisation Electrotechnique) (Europe)[2]
- Digital Video Broadcasting (DVB) and Digital Audio Video Council (DAVIC) (international)[3]

This list is by no means exhaustive, and other bodies such as the U.S. CableLabs[4] play an important role in the standards arena. CableLabs administers development of specifications within a consortium, Multimedia Cable Network System Partners L.P. (MCNS).[5] MCNS members are U.S. cable operators.

Two important issues arise. First, there is currently a lack of coordination between the various standards bodies. There is liaison between IEEE 802.14 and the ATM Forum, as well as between IEEE 802.14 and DAVIC, and DAVIC and DVB, but there is as yet no single body accepted by the worldwide CATV community, especially for residential systems. Second, much of the effort in the various standards bodies is based around standardization at the physical layer: modulation, transmission, coding, and signaling. While there is some network management activity (notably within CableLabs/MCNS [1]), this concentrates on management of the network elements (e.g., cable modems) and radio frequency (RF) interface rather than management of network services as a whole. However, the lack of standardization in network components and architecture may not be as bleak for network management as it first sounds if the higher (data link and network) layers of the network architecture are to follow existing standards (see below).

CableLabs is seen as the most important body within North America. Outside North America, DAVIC is considered the key player. DAVIC seeks not to define new standards, but to rationalize and harmonize the use of existing or emerging standards.

Network Structure

Network structure varies not just across the Atlantic divide, but also within Europe. For example, the Benelux countries (Belgium, Netherlands, Luxembourg) have mature coax-based networks. These were (in general) deployed after being carefully planned and designed with the specific requirements of delivering only analog broadcast television services. It will be challenging to adapt these networks to provide digital services. In contrast, the United Kingdom has many new CATV networks being developed with digital backbones, using synchronous digital hierarchy (SDH), which have the potential to offer huge amounts of digital capacity. In this section we examine the network technology in CATV networks and how it affects network management requirements. Excellent expositions of the technology issues concerning North America were presented in [2, 3]. In Figs. 1 and 2 we show a typical scenario of how the network technology is evolving in Europe. Figure 1 shows the current state of mature/traditional networks in Europe. Figure 2 shows a scenario for evolution to FSNs that supports digital transmission.

We note the following features for the network of Fig. 1:

---

[1] *http://walkingdog.com/catv/index.html; http://www.atmforum.com*

[2] *http://www.etsi.fr; http://www.cenelec.be*

[3] *http://www.dvb.org; http://www.davic.org*

[4] *http://www.cablelabs.com*

[5] *http://www.cablemodem.com*

- The network consists mainly of passive components (amplifiers)
- The amplifiers are capable of relaying signals in both directions.
- The network topology is tree-shaped, branching out from the head-end, reflecting the usage of the network (i.e., analog broadcast services).
- The set-top box simply acts as a tuner or channel selector for the TV, but may include some analog access control mechanism for pay-TV channels.
- The network is effectively a shared media system which is contention-free at present (only one transmitter, the head-end), but will not be contention-free in the future (with interactive digital services and data services) unless a media access control protocol is used.

A key distinction between many of the North American networks and the European networks is the use of the return path on the existing coax plant. The North American networks often do not have bidirectional amplifiers installed, or, if they are installed, they are not enabled. Thus, the return path from the user is via a PSTN connection — the *telco return*. This severely reduces the *symmetric* broadband capability of the North American networks but still allows useful *asymmetric* services such as information download — "Web surfing" — which need larger downstream capacity. However, the application of such networks is obviously limited.

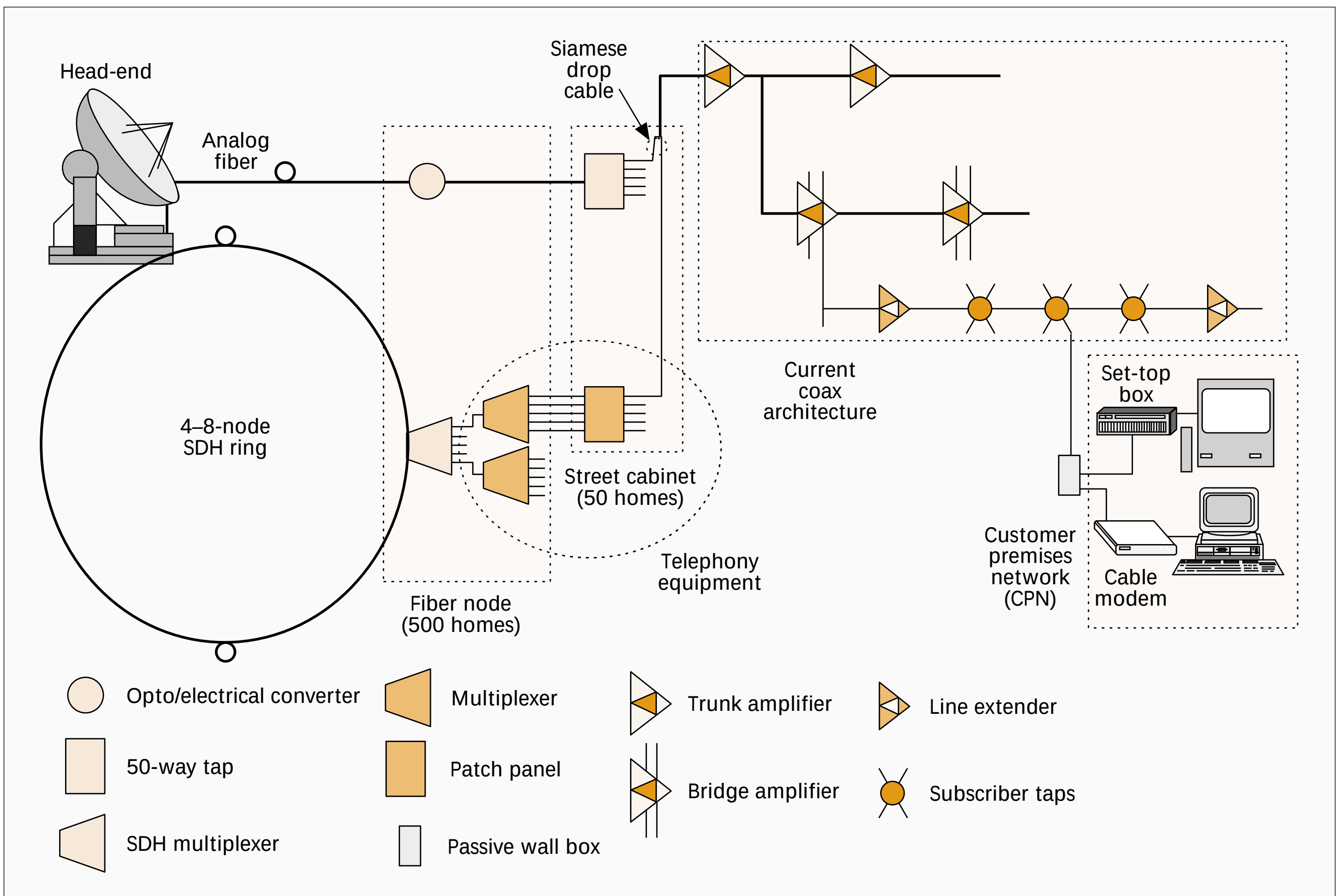
Many CATV operators also offer supplementary services, and these will be discussed later. From the point of view of network management, these networks do not have many active components that can be managed remotely via an automated network management system. It would be useful to have some sort of fault management facility in the set-top box and possibly in street cabinets, but generally the network operator relies on feedback from customers to detect operational errors and isolate faults.

With the introduction of a digital data channel on the return path, however, there may be a need to apply some sort of media access control. For network management, there may be a more fundamental need to remotely disconnect certain users from the network when they are not using the return path, for instance, to combat noise ingress (see below).

For the network of Fig. 2, we note the following:

- There are now many active elements in the network such as digital multiplexers and switches.
- There will now be active software components within the network that require management.
- The network carries both analog and digital streams.
- The local delivery of digital transmissions is via the existing coax infrastructure.
- In the network shown, a United Kingdom scenario, the telephony is delivered (effectively) via a separate network due to regulatory requirements.
- There is now both a digital and analog termination/adapter in the home.
- For the digital streams in the local/neighborhood area, the network is still seen as shared media access.

Figure 2 is an example of a fiber-reinforced network or hybrid fiber coax (HFC) network. Note that the fiber shown in this type of network is usually run in pairs, for both the analog part and the SDH ring. In fact, there are many different architectures for HFC networks. This architecture could



■ Figure 2. *A representation of evolution to HFC networks.*

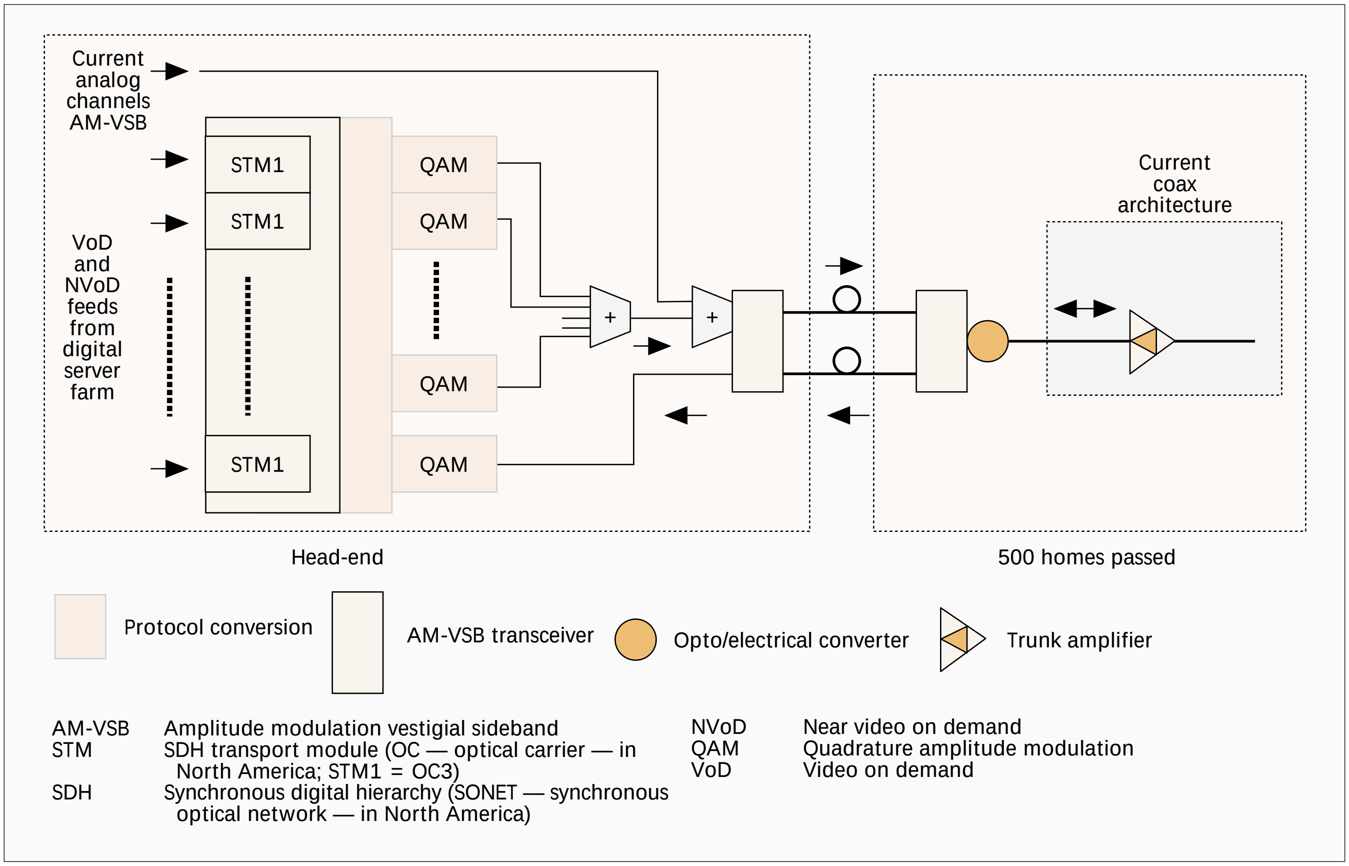


Figure 3. *An FSN head-end with digital capability.*

obviously be extended to provide data services using ATM, provided that a suitable physical layer delivery can be found for the coax part of the network. This setup is also known as fiber to the neighborhood (FTTN). Many of the management tasks here are actually service management issues and will be discussed later.

At the head-end, support for the digital part of the network might typically be realized as shown in Fig. 3. In fact, Figs. 2 and 3 depict an interesting scenario. In this case, the digital SDH carrier is being used solely for telephony while the current coax/analog architecture is being used for digital data! In many cases this is due to the lack of an integrated carrier such as asynchronous transfer mode (ATM). Of course, since ATM equipment is now widely available, the maturing FSNs can take digital feeds from the head-end directly to the SDH carrier with conversion at the street cabinet.

The *server farm* of digital video servers would require careful management to perform such functions as load balancing and failsafety, to provide the best utilization of the resources available and a reliable service. This would be especially crucial if the servers were expected to run at relatively high loads to increase their cost effectiveness. The communication architecture for clustered server technology is still evolving, and their management needs have not yet been clearly identified.

The quadrature amplitude modulation (QAM) functions would probably be realized as a bank of modems that would also require (at the very least) monitoring to preempt any faults or detect the presence of particularly error-prone channels. If ingress (or other noise) is a problem, the management actions here might involve signaling/interaction with other components such as amplitude modulation vestigial sideband (AM-VSB) transceivers in order to select less noisy channels. This means that the AM-VSB transceivers must be capable of being managed dynamically and in real time. This dynamic channel selection may also apply to the cable modem at the customer premises network (CPN), so there is a need for this device to be manageable also.

The fiber node and street cabinets provide local distribution points for around 500–1000 homes. With the setup shown in Fig. 2, this could be a passive device. However, it would still be useful to have information such as error rates, signal-to-noise ratio (SNR), and usage statistics for the area covered by the fiber node to preempt possible fault or loading conditions. In the future, the fiber node and street cabinet may support fiber to the curb (FTTC) or fiber to the home (FTTH), so the importance of this device in terms of management will increase. Also, the equipment at these points may become more complex (especially the street cabinet) if ATM is used to deliver to the set-top box or cable modem. In these cases, more sophisticated management facilities will be necessary.

In terms of network management capability, there are standards to support management of SDH [4] from the International Telecommunication Union (ITU), and support for management of ATM network elements from the ATM Forum [5], as well as from the Internet Engineering Task Force (IETF) [6] and ITU [7]. However, management requirements of (and management information models for) the QAM components and lower-layer support functions (modulation, transmission, coding) have yet to be realized. Another technology used, predominately in the return path, is quadrature phase shift keying (QPSK), which also lacks standardization activity with respect to network management.

More detailed coverage of some of the broadband network management issues is presented in [8].

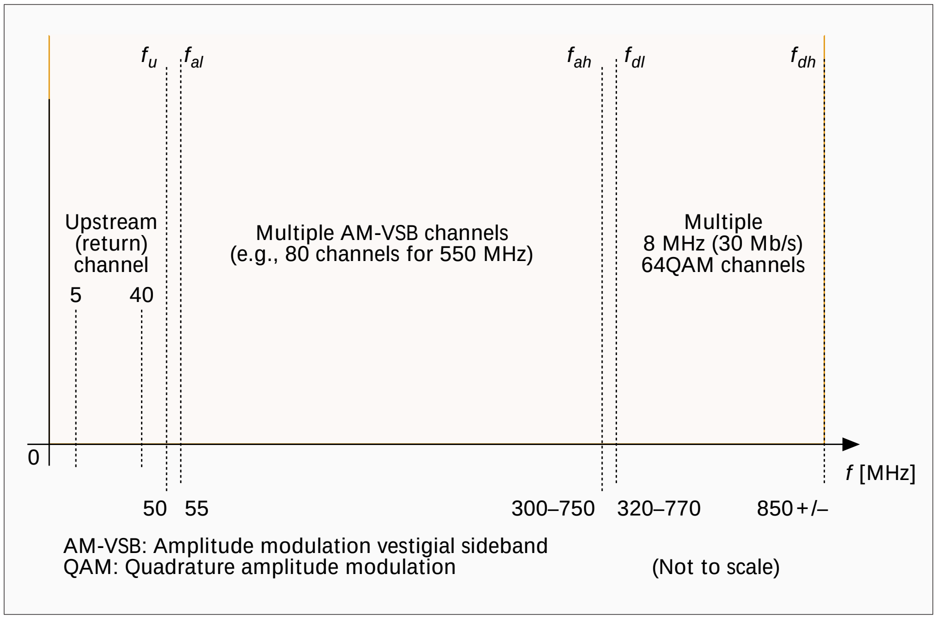


Figure 4. *Typical RF spectrum usage in CATV networks.*

Radio Frequency Spectrum Usage

A typical snapshot of the spectrum usage in CATV networks is depicted in Fig. 4. We note the following:

- This whole spectrum is seen throughout the network, including at the boundary, within the CPN. Here, by CPN, we mean the network at the user's premises (i.e., the network devices connected to the provider network; Fig. 1).
- The available bandwidth for the upstream channel is in the region up to 50 MHz. The CPN will use a 2 MHz channel, typically between 5 and 40 MHz. This may change in the future, especially with the introduction of digital channels at the higher end of the spectrum, or with the use of different modulation schemes.
- The CPN using the return channel is effectively on a separate network and does not share bandwidth with any other cable traffic.
- There are several bands around 27 MHz allocated for use by citizen band (CB) radio, and their exact use within the CATV network is presently unclear. It is likely that they will be reused as part of the return path.
- Some of the coax-based infrastructure in Europe contains installed amplifier components that cannot amplify in the lower bounds of the upstream region or in the upper bounds of the downstream region.
- It is very unlikely that, in the short to medium term, the bandwidth used for analog transmission will be released. Analog programming will continue while digital technology remains at its present (relatively high) cost levels; there is a large installed base of analog equipment that would need to be replaced.
- The networks are unlikely to change to baseband transmission in the short to medium term

Data access to the CATV networks will (initially) be via a RF modem that operates in the 5–40 MHz region. The region from f_{dl} to f_{dh} will be used for the new digital channels to be introduced. Current plans are to use these for digital TV. However, because these channels are seen at the CPN, provided an economical RF modem solution can be implemented, some of these may also be usable for data (e.g., for a separate downstream data channel). The exact values of f_{ah}, f_{dl}, and f_{dh} depend on the particular capabilities of the network.

There is a need to manage this bandwidth, possibly in a very dynamic way. There is currently a lack of standards (or even general agreement within the CATV industry) on how the spectrum should be used. It is imaginable that different CATV operators with different customer needs may want to try to make use of the analog and digital channels in a very flexible way. Indeed, the operator may wish to decide which parts of the spectrum to allocate to analog channels and which to digital channels. This needs to be addressed by the management system.

Ingress Noise (Ingress)

When the return path is on the existing coax plant, rather than by telco return, there is a problem of ingress noise. Users expect to connect their CPNs directly to the operator's network. Not only will each additional CPN add its own noise component; there is also the danger that some individual users may have particularly noisy (e.g., faulty or old) equipment that brings the SNR on the main network to an unacceptable level. This problem will be much more acute with all-coax networks, so there is a need for intrusive management to be able to monitor the noise from individual CPNs and for a CPN to be controlled (i.e., disconnected!) from the network if it is too noisy. This is a very sensitive point, both technically and politically. Technically, there are requirements for:

- *Restricting noise ingress onto the network in the first place:* This requires the use of a physical medium access control system, say, some sort of dynamic switch at the CPN. The network would only be physically connected to the medium when it needs to send or receive data. This may restrict throughput to the physical switching speed of any particular hardware.

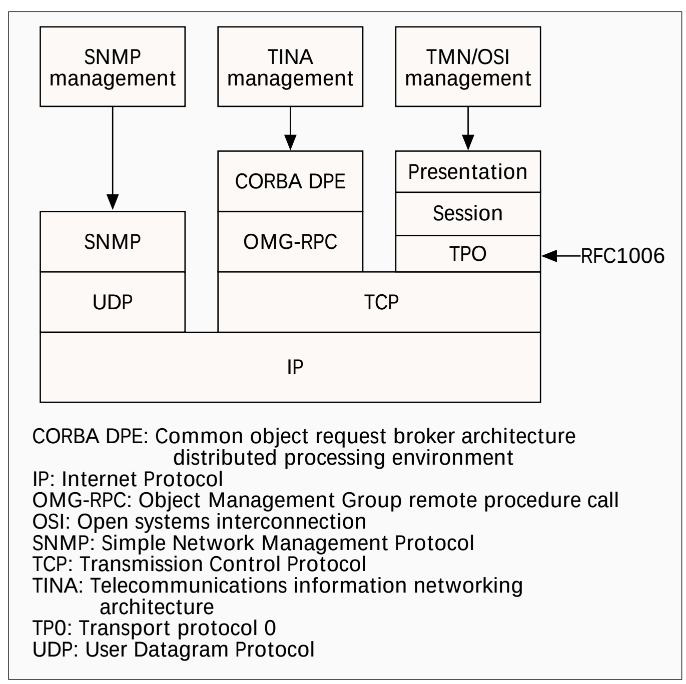


Figure 5. *United by IP: a multiplatform management scenario.*

- *Detecting that there is too much noise on the line:* This should not be too difficult, and can be done by simple monitoring equipment.
- *Isolating the source of the noise:* Ideally, one might want to detect the device causing the noise and ask it to be less noisy! However, it may be hard to determine the single device causing the noise and may be necessary to disconnect a whole CPN. Indeed, the noise might not be caused by the devices connected to the CPN itself but by other electrical and RF signals (motors in washing machines etc.). Again, the solution here might be to allow network management systems to remotely disconnect the CPN from which the noise is occurring.
- *Existing network legislation:* In some countries (e.g., the United Kingdom), it is required that telephony services be available at all times for emergency use. Therefore, there would need to be (physical) isolation between data service provision and telephony service provision if ingress control actions such as disconnection were being considered. (Indeed, this is depicted in Fig. 3; the Siamese drop cable is coax wrapped in twisted pair.)

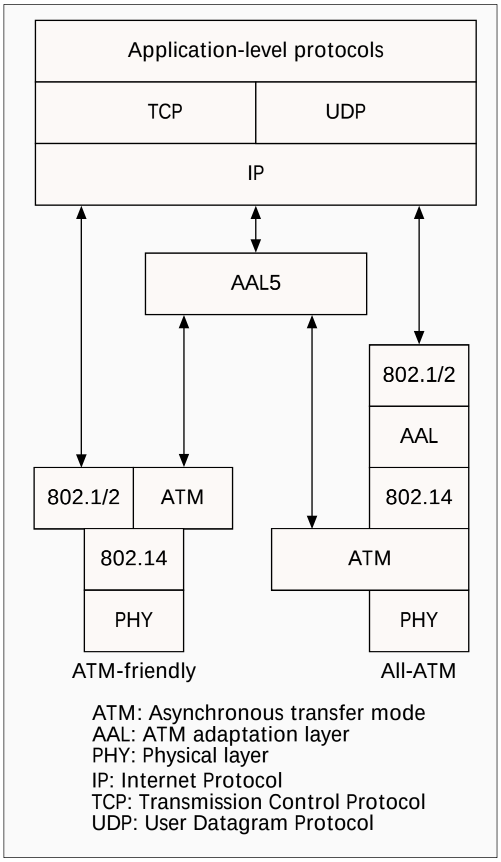
Two important political issues are:
- *Does the provider have the right to disconnect a subscriber?* It might be argued that it is the responsibility of the operator to reduce the noise in the network and should not be a concern of the subscriber.
- *Who owns the network termination point?* Currently, most CATV companies in Europe provide the set-top box, and it does not belong to the subscriber, but in North America the set-top box can be built into the TV set. If the CATV operator is disconnecting the CPN, will it in fact need access to the set-top box to perform this task? Otherwise, will the CATV operator have to build a new network termination that is an active box to which the CPN connects?

It can be seen that the technical issues are likely to be directed by resolution of the political issues.

Standards for Network Element Management

Currently, there is a lack of standards for the network elements in CATV networks. There is no agreed standard definition for the core functional components for the head-end. This means that management of the services and network could well be ad hoc, based solely on whatever facilities are provided by the equipment manufacturer. The street cabinet and fiber node have no standards for remote management. Currently many of them may be passive devices (as in Fig. 1), but if they were to become active network devices (Fig. 2) it would be essential to have remote management capability.

The picture is not so gloomy for SDH and ATM equipment. There are standards available from the International Organization for Standardization (ISO)/ITU [4, 7] as well as the ATM Forum [5] and the IETF [6].



■ Figure 6. *Possible protocol stack scenarios for CATV FSNs.*

However, the main problem will be how to obtain an integrated management environment that encompasses the *network* management requirements, as well as the *service* management requirements of future FSNs. By service management we mean not only the management of the *data* delivery service (offered by ATM, SDH, and RF systems), but also the *content* delivery service as seen by the customer.

The Communications Protocol Stack

The various network components and management systems will need to communicate, so there must be support for a common underlying protocol stack. A good choice here would be the use of IP as the lowest common denominator for a network-level (level 3) protocol. The main advantages of using IP are:
- It is likely that IP connectivity will be offered as a service to subscribers, and thus will be provisioned by CATV operators (or allied service providers) anyway.
- It is a well known, well understood, widely used, open, and robust protocol suite.
- It allows the support of several infrastructures for management needs, such as SNMP [9–11], open system interconnection (OSI)/telecommunications management network (TMN) management [12, 13] (by use of RFC1006 [14]), and Telecommunications Information Network Architecture (TINA) [15] based on common object request broker architecture (CORBA) [16] systems using the Object Management Group (OMG) remote procedure call (RPC), as depicted in Fig. 5. This covers (currently) the most popular standards for open management (!), and can be considered a safe bet for the foreseeable future.

However, IP itself needs to be carried in whatever is present at the data link layer (level 2). Figure 6 shows how this would be possible for a HFC-based network using the IEEE 802 or ATM Forum Residential Broadband Working Group (RBB WG) specifications. The IEEE P802.14 and the RBB WG have been looking into the provision of broadband capability in the same domain as CATV networks. Most of the current work focuses on the provision of ATM services on HFC networks. A summary of the 802.14 work is presented in [17], which also states that the two competing protocol stacks are as shown in Fig. 6 (the "ATM-friendly" and "all-ATM" stacks), suggesting that the ATM-friendly stack is likely to be chosen since its access interface is consistent with both the ATM Forum and IEEE 802 LAN models. This would also then allow easy transition of IP applications onto such networks, and allows for a neighborhood LAN model. In Fig. 6, the upper part of the diagram has been added to show how IP would be provided at the appropriate interfaces. IP would be able to work over either stack, although in the all-ATM stack, the ATM interface may not be available as depicted. An alternative would be to use the ATM Forum's

LAN emulation (LANE) [18]. This would allow coexistence of the various network protocols and promote interworking, but possibly at some cost in efficiency. The use of LANE may also be beneficial if it allows the integration of work in progress for allowing use of virtual LANs (VLANs) and multicast (IEEE 802.1Q) as well as some quality of service (QoS) mechanisms (IEEE 802.1p).

IEEE 802.14 work currently recommends the use of 2 MHz channels using quadrature phase shift keying (QPSK) for upstream. The noise regime in the upstream (return) path does not permit the use of 64QAM as for the downstream path. However, there are other suitable technologies for use in the CATV environment. Currently, synchronous code-division multiple access (S-CDMA) and multicarrier modulation schemes are receiving attention for possible standardization at the physical layer.

At the time of writing, the ITU had almost approved Recommendation J.112 for the physical layer. Unfortunately, it has three Annexes, A, B, and C, specifying technology favored by Europe (based on DAVIC specifications), North America (based on CableLabs/MCNS specifications), and Japan (a modified version of the CableLabs/MCNS specifications), respectively. However, it is entirely possible that European operators will buy cable modems from North American manufacturers conforming to the North American version of J.112 rather than the European version.

So it may end up that there is not much difference between the North American and the European networks at the physical layers — but the operators are still unsure about the evolution of the technology!

The Need for a Common Carrier

CATV network operators still envisage that their main business will be the provision of entertainment services. This means movies and other TV programs, but with more controlled delivery, such as video on demand (VoD) or near VoD (NVoD). For CATV operators, it therefore makes sense to have the network optimized for the provision of video streams. However, for data services running over IP, it is desirable to have the network optimized for the provision of packet data services. MPEG-2 streams appear to be the "natural" choice for entertainment programming, but ATM is considered to be a more general technology, and so more suitable for the long term in enabling CATV networks to become FSNs. Thus, there are proposals for offering interfaces for both types of carrier, by allowing MPEG-2 over ATM or ATM over MPEG-2. An analysis of these two scenarios is presented in [19].

It seems clear that IP will play an essential part in the DAVIC model, being used for application-level signaling and network management. Also, the provision of IP services for subscribers will be a major consideration. It seems sensible, therefore, to use underlying communication infrastructure that is not only optimized for delivering entertainment services but will support IP with good performance. Furthermore, while IP is a major data communications technology, a network operator may wish to offer other data communications capability in their FSN; therefore, multiprotocol capability will be important, so ATM would be a more natural choice.

Also, an FSN may wish to provide data communication services to allow access not just within a community/city area but on a national or global scale (i.e., allow users of its services to access widely distributed resources and communication points). This may involve the need to interwork with a telco, and thus the need for some sort of gateway function. This may be eased if the CATV community uses a similar level 2/3 technology to that of the telcos (e.g., ATM).

One could consider that this is simply an interface issue — why not offer ATM over MPEG-2 as an interface and still use MPEG-2 as the level 2 carrier? This is indeed possible; however, there may be complications when IP assumes that ATM-based signaling (e.g., Q.2931 [20]) and ATM-based switching is being used in the network. (There is currently work in progress to map IP "signaling" protocols such as the Resource Reservation Protocol, RSVP [21], and ST2+ [22] onto Q.2931.) Therefore, such services would need to be mapped onto MPEG-2, which would be a major task, if indeed not found to be infeasible.

For these reasons, it seems logical to use ATM as the common carrier at level 2. Since ATM is a general networking technology, it would seem logical to use ATM as the carrier of choice within the CATV network, with the use of MPEG-2 over ATM where required for entertainment services. While MPEG-2 could be made to carry all the traffic types listed above (including entertainment), there would be a large amount of work needed to provide x-over-MPEG-2 solutions, while x-over-ATM solutions — notably IP over ATM — already exist or are being examined closely. Further work on developing the use of Internet protocols to run over ATM will continue within the Internet community, and the CATV community would simply need to adopt this work and could use it easily. The same would not be true for using IP over MPEG-2, since there is no activity within the IP community for carrying IP within MPEG-2 streams. If ATM is widely adopted by the CATV community, they may need to expend little or no effort in porting IP-based applications for use on CATV networks.

From the management perspective, SNMP allows the management of IP-based resources, including protocols and devices. There are also SNMP management information bases (MIBs) defined for ATM equipment. However, there are no such management standards for MPEG or MPEG equipment, so the choice of network protocol would seriously affect the management of the network.

Service Management

Here we are concerned with management of the services seen by the CATV customer. The key to the success of FSNs is the provision of a diverse and useful range of services to the customer in a flexible manner. Examples of such services are VoD, interactive TV, teleworking, distributed games, and video telephony. These services are complex in nature, and the way in which the CATV community wishes them to be accessible also leads to complexity in their provision. There may also be a requirement for the provisioning of social services such as remote wardens and access to online public access catalogs (OPACs). The CATV community would like these services to be accessible dynamically and easily to subscribers from their home. The subscriber would be able to choose a service (e.g., a feature film from a VoD library), pay for the service online, and then receive that service immediately. The services a subscriber selects or browses will be distributed in nature, so the platform used to offer the services should try and hide technical details, such as network-specific details of the resources required to provide particular services (location, network topology, addressing details, etc.). The process of service selection involves the service platform offering a one-stop shopping service:

- *Service selection:* The subscriber is able to browse or review services on offer.
- *Provider selection:* The subscriber is able to select between different providers offering the same service.

- *Genericity:* Services are presented in a generic way but with specific information available.
- *Real time:* Service can be selected immediately.
- *Payment:* The subscriber is able to pay for the service online.

To illustrate these points, imagine a home movie service offered to subscribers over the CATV network, using the handset and some menus appearing on the TV screen:

- *Service selection:* The subscriber is able to see the menu of movies available, and perhaps watch some trailers or previews.
- *Provider selection:* The subscriber can choose the same film from several different providers of the same movie (in the same way s/he might choose between different video rental shops).
- *Genericity:* The subscriber sees the services presented as a home movie service, but specific details are presented when a certain service or provider are selected (e.g., price, availability).
- *Real time:* The subscriber selects a movie to watch immediately with fine-grained control of content presentation and delivery (VoD), or almost immediately with no real control of content delivery (NVoD).
- *Payment:* The movie is delivered to the subscriber as soon as payment (or at least the ability to pay) has been verified electronically, via the handset and other security information (smart card, PIN number, etc.).

The architecture chosen for service provision will have a strong influence on the management system, since the service model may be quite sophisticated. It seems very important in this case that the service architecture and management system are not completely divorced during the design of the system. In this section we look at the contenders for the network management platform of choice. In fact, DAVIC (currently considered the major player outside North America in the race to produce a service architecture for the CATV community) has chosen to use a TINA/CORBA distributed system within a Java-based execution environment.

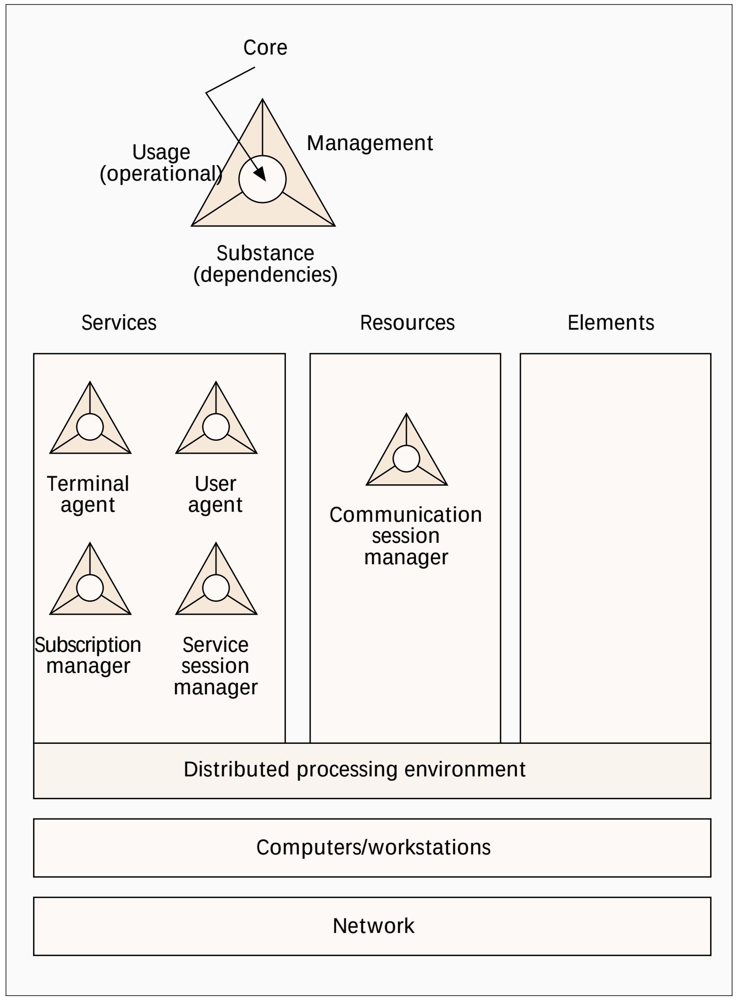


Figure 7. *The TINA component model for distributed applications.*

A more detailed description of the individual technologies listed in his section can be found in [23].

SNMP

SNMPv1 [9] is the de facto industry standard for open network management. This is the management architecture produced by the Internet community. It is used extensively and with great success in the management of network elements because of its simplicity and lightweight architecture. However, it uses an unreliable transport protocol, and even with the advent of functions such as the INFORM message in SNMPv2 [10], may be considered unsuitable for network or service management across the wide area without the support of reliable network connections. Its simple information model would make it hard (but not impossible) to perform complex service-related tasks. SNMP also lacks a distribution model that is akin to a true distributed system, relying on knowledge of the IP addresses of SNMP agents and managers in order to function. The lack of security in SNMPv1/2 and the development of a better-defined application architecture is addressed in the SNMPv3 work [11].

With the sophisticated information services being planned and defined in an object-oriented fashion using the CORBA Interface Definition Language (IDL), such a simplistic information model as that offered by SNMP might be considered to be insufficient for the management of the application services based on CORBA. However, this has not prevented DAVIC from creating SNMP MIB definitions for the management of network components [24, 25]. It remains to be seen how DAVIC intends to integrate this into their general management architecture in combination with the architecture adopted for service management.

OSI Management and TMN

The TMN uses OSI management technology within a well-defined framework to offer network-element- and network-level management capability. These standards are output from the ISO and ITU. Although the use of this technology is meant to extend to service- and enterprise-level management, this remains mainly an area of research. However, there are standard definitions for managing SDH [4] directly, and ATM both directly [5, 7] and via SNMP [5, 6] by use of special Q-adapter (proxy) functions [26]. (The ATM Forum defines both OSI and SNMP management capability [5].) The key value of this technology is that it is now fairly mature, and there is a lot of experience in its use. Also, it is much favored by the major telecom operators. However, it is considered very heavyweight for smaller network elements, and is much more expensive than SNMP technology. Here is where the use of SNMP proxies has great value — using simple, inexpensive, lightweight SNMP agents on the network elements and using an OSI proxy agent to present a network-level abstraction of the network elements. The use of TMN

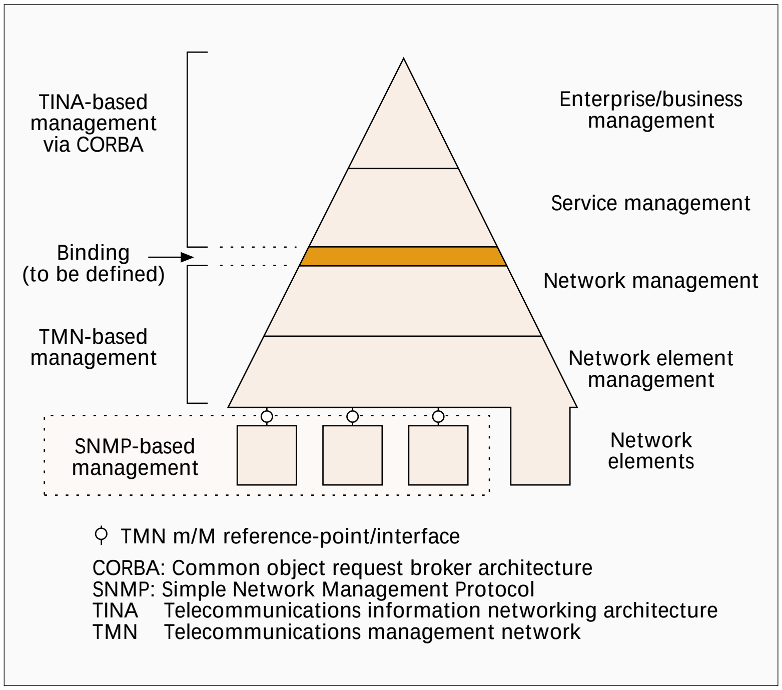


Figure 8. *Three-tier integrated management scenario.*

for the management of application services has received some research, but is not generally well investigated. However, its use in the management of telecommunication systems is well understood.

The TMN uses the OSI management model, which is a client/server-based model, using an object-oriented information description language (which can also be used within the TINA framework). In fact, it seems possible to offer a CORBA IDL-based interface to the TMN for service management (see below).

TINA and CORBA

TINA is an initiative that seeks to define a general computing platform based on a standard software architecture. It does not (yet) seek to define another set of network management or communication standards, but to offer a framework in which to unify the best parts of the existing standards. TINA is not specifically a management architecture, but tries to define an overall component methodology for building distributed systems. Although the TINA principles could be applied to TMN service management, it seems most likely that TINA will be deployed using the distributed environment offered by CORBA-based systems. TINA is designed with the particular goals of service management in mind. It does this by abstracting away from the network details, such as topology and location of resources, relying instead on the provision of a standard distributed processing environment (DPE) to hide these details. (The DPE abstraction comes from the ITU Open Distributed Processing Reference Model.) It is particularly geared to service management by design and so might be considered most suitable for use as a platform for implementing the distributed services that the CATV community envisages for FSNs. The TINA overall architecture is based on a service component model, as shown in Fig. 7. A key feature of the TINA service component is that it has an integrated management architecture [25], with each service component offering a management interface. This promotes an integrated service management approach. The same is not necessarily true in the development of Internet or OSI services, in that the service components are divorced from the management components of the application model. There is a possibility that the TINA principles can be used without implementation of the TINA architecture reference points. Work on use of TINA[6] seems to indicate that TINA can provide useful functionality, although management aspects are still not fully investigated.

The roles and operation of the service components in Fig. 7 compare well with our description of the desired subscriber-service interactions envisaged for FSNs in the CATV community (see the beginning of this section). The *terminal agent* is the interface through which the subscriber/user interacts with the rest of the system. This function would be provided by the handset and the TV screen. The *user agent* holds information about the subscriber, such as personal details and credit rating. The subscriber may request a service that would be checked by the *subscription manager*. This would be followed by further interactions between the *service session manager* (to invoke the service) and the *communication session manager* (to initialize and maintain communication resources for the session), eventually resulting in the service appearing at the terminal agent. The interactions of the user agent, subscription manager, service session manager, and communication session manager are transparent to the subscriber.

TINA management [27] addresses two broad areas, *computing management* and *telecommunications management*. Computing management deals with the management needs of real resources such as computer hardware and platform, and tackles generic issues such as configuration and instantiation of software, and management of the DPE and computing environment.

A Possible Management Scenario

Currently, TINA is not complete (final architecture due soon), so it is still hard to envisage the exact way it will be deployed. The issues of service and enterprise management it is designed to tackle are still research areas; however, it seems that the technology is promising. Meanwhile, there is much experience and knowledge in the use of TMN/OSI and SNMP management, and it does not seem reasonable to throw away this expertise and installed base, especially if it is known to perform useful management functions for network element and network management. The TINA architecture does not preclude the use of TMN; indeed, the information modeling in TINA could well be achieved by the use of GDMO [28] as used in TMN. A possible scenario for usage of the TINA architecture that embraces the current TMN technology but also utilizes a CORBA-based system is depicted in Fig. 8. In this scenario, the existing knowledge base of TMN is used for the purposes of network management. Integration of SNMP network components can be achieved using OSI-SNMP proxies in the TMN environment. New services and their management systems are built using the TINA approach and the service component concept.

This allows existing and legacy management infrastructure to be maintained, but allows new services to be designed and introduced easily. The key to this scenario is the binding between the TINA/CORBA and TMN domains, which is currently being researched [29].

[6] *http://www.tina97.cl*

The DAVIC Framework

DAVIC is a consortium of industry players in the CATV arena (manufacturers, CATV network operators, service providers) who are looking to standardize a service and management system for use in CATV networks for the delivery of all kinds of digital services. DAVIC is keen to see CATV operators become FSNs. The work of DAVIC seeks to provide a framework in which existing and emerging standards can be used in a unified way within CATV networks. One of its main goals is to try to have no optional technology choices for a particular function in order to ease progress, implementation, and interoperability. DAVIC has produced v. 1.0 of its recommendations [25], which are concentrated on the aspects of physical connectivity (level 1) and the transmission technology. There is still much work to be done, and as with all such newly formed consortia, there have been some political and technical setbacks.[7]

In the authors' view, the issue of management is still somewhat confused in DAVIC. SNMP MIBs have been defined for some basic management functions [24]. However, the consortium seems keen to adopt a TINA architecture using CORBA as the platform for the implementation of its services. This would suggest that there is a need to consider the kind of scenario described in Fig. 8, with SNMP integrated via TMN for management of network components, and TMN "glued" somehow to the service management features implemented using CORBA. Although it would be possible to design a system to integrate SNMP components directly into a CORBA framework, the SNMP architecture lacks the richness of the TMN architecture, has poor security in versions 1 and 2, and may be unsuitable for use in some wide-area scenarios.

The IETF IPCDN WG

The Internet Protocol over Cable Data Networks (IPCDN) Working Group[8] is looking at the provision of IP services over CATV networks. Its main concern is with the definition of a standard to allow IP to be transmitted and received over the CATV infrastructure. It is not concerned with higher application services, but its output may be important if IP is indeed adopted as the common level 3 network protocol. The IPCDN WG has liaison with US CableLabs, and is currently trying to establish SNMP MIBs for the management of the RF interface, cable modem, and cable modem termination devices, and IEEE 802.14-based IP subnetworks. At the time of writing, these MIB definitions are currently at the Internet draft stage, and it is anticipated that they will be issued as requests for comments (RFCs) soon, but the WG has been subject to delays.

US CableLabs

US CableLabs (Cable Television Laboratories Inc.) is a consortium of U.S. cable TV operators involved in a collaborative program of R&D in order to help the CATV companies move into the wider telecommunications and data communications arenas. CableLabs has been active in trying to get agreement on standards for the CATV community via a process of acquiring input using requests for information (RFIs) and requests for proposals (RFPs). CableLabs has made progress on many items concerning the lower-level cable infrastructure, but also has a "bottom-up" approach and has yet to address the problem of integrated network and service management. However, they have at least managed to define many aspects of the functionality of various parts of a CATV network. This is the first step in defining network management requirements and management functionality. CableLabs and IPCDN are working closely to establish SNMP MIBs, as mentioned above.

Europe has no counterpart to US CableLabs, but there is currently activity to establish Euro CableLabs.

Security

With the service model described at the beginning of this section, there is a need for a dynamic and flexible security architecture. When a subscriber wishes to buy or use a service, security mechanisms must be in place to allow:

- Authentication of the subscriber: This would require the use of some sort of certification authority, possibly realized as an online service.
- Access control: Check any access control permissions that might apply to that subscriber with respect to their service request.
- Payment: Validate electronic payment from the subscriber, or at least check the subscriber's ability to pay.
- Subscriber security: Accommodate security requirements that the subscriber might have (e.g., the subscriber may want anonymity in use of the service), as well as provide protection of sensitive information such as credit card numbers, passwords, and so on.
- Secure service delivery: Deliver the service to the subscriber in a secure manner if required; for example, if it is a pay TV channel, delivery of the channel to the subscriber should be on an encrypted stream that cannot be observed by other subscribers who have not paid for that channel).

There are additional security requirements for the network operators who wish to protect their network resources and the information on their servers (e.g., movies and other content) from being accessed by subscribers or nonsubscribers who have not paid.

The management system should be at least as secure as the system it is trying to manage, or a possible attacker may be able to obtain access to services or sensitive information (such as subscriber records) via the management system rather than by attacking the system directly.

The Internet community offers no agreed security mechanism for SNMPv1 and v2. SNMPv3 specifications include security specifications, but the SNMPv3 architecture requires that SNMPv1 and v2 entities be modified in order to use the new specifications. However, security mechanisms have been specified for IP itself [30]. For TMN, at the time of writing work was work in progress to ratify security standards within the ITU. There have also been some practical experiments to show that fairly realistic secure management with TMN is possible [31, 32].

At the time of writing, TINA does not (yet) specify a security architecture; however, CORBA has specifications for supporting secure transactions. The lack of an overall security architecture is a major drawback for use of this technology for the provision of services, as well as for the provision of management capability. It can be seen from the points listed at the beginning of this subsection that security mechanisms are essential in order to allow services to be sold dynamically and in real time over the network. In the interim, it may be possible for such systems to exploit the

---

[7] *Two examples of such setbacks: 1) DAVIC has selected two possible level 2 carriers, ATM or MPEG-2, breaking its own rule of "no options"; 2) at one point, a "karaoke-on-demand" service was given a much higher priority than the provision of IP services!*

[8] *http://www.ietf.org/html.charters/ipcdn-charter.html*

security mechanisms in the underlying technology (e.g., IP). However, these security mechanisms are concerned with security of the communication protocol and do not necessarily offer the functionality required for application-level (service-oriented) security such as that required for service provision or service management.

North America vs. Europe

One major issue in selecting a management platform or technology is the (often religious) attitudes toward technology that have been evident on both sides of the Atlantic. Many Europeans ignored the SNMP technology, while many North Americans were not happy to consider the OSI/TMN-based approach. Both technologies have a role in a large heterogeneous network environment, and they will have to coexist. This technopolitical stance has now mellowed somewhat, and there are now companies on both sides of the Atlantic actively developing and selling products that incorporate both technologies. The use of CORBA appears to have gained equal acceptance on both sides of the Atlantic, and it is yet to be seen if the TINA architecture and principles also find favor, but certainly there seems to be great momentum in the TINA camp.

However, current trends seem to indicate that there could again be a polarization of technology, with the North American networks adopting the SNMP approach as put forward by the current CableLabs/MCNS/IPCDN work, while Europe will integrate the SNMP technologies under an OSI/TMN approach.

The authors consider the best scenario for both sides of the Atlantic to be that depicted in Fig. 8, using the best tool for the job at the appropriate place in the FSN.

Summary

The CATV companies wish to become FSNs and offer a whole host of digital and data services. However, much of their networks at the moment consist of analog transmission services, and the services themselves are analog (e.g., TV and satellite channels). There are some newer networks using SDH that have the potential to offer digital services, but these are not heavily deployed. Therefore, there is a need to gradually introduce digital services without disrupting current analog programs. With the introduction of new technology, the CATV networks will have more active components than at present. This not only includes network devices but also application services such as video servers and other information servers. The analog-to-digital migration path requires careful management of physical measures such as electrical bandwidth and noise, as well as these new active components (both hardware and software).

The CATV industry needs to better define the functional parts of the CATV network (e.g., the head-end and distribution points) so that network management requirements and (ultimately) management functionality can also be defined. This should also provide the CATV community with a framework in which to deal with aspects of network management which are specific to CATV networks, such as noise management and (electrical) bandwidth/channel management.

The technology chosen to implement the services within the CATV community will strongly influence the choice of network management technology. If systems are based on current technology (SDH, ATM, and Internet protocols such as IP, TCP, and UDP), there is already a wide knowledge base for, and expertise in, the management of network elements (based mainly on SNMP) and wide-area network management (based on TMN/OSI). Service management techniques are now developing for and activity is currently based on the use of the TINA architecture implemented in CORBA. The use of TINA allows integration of management systems with service provision.

The use of IP plays a vital role as a common underlying protocol to allow the coexistence of all these management systems. Its use would also be welcome because it is heavily deployed throughout the world and there is a lot of expertise in using IP. Also, there is a large installed base of management systems using network element management and network management based on SNMP, the most widely used open network management system.

Ideally, the CATV companies would like to have integrated service provision, service management, and network management so that the control of the network and the services offered can be handled from one platform. However, the use of standard network and systems management technology is currently in a fragmented state. Much network element management is achieved using SNMP, by far the most popular system because of its simplicity. However, SNMP can be inadequate for certain wide-area network management scenarios. Many telcos use TMN/OSI management in the wide area. This technology has now achieved a degree of maturity, and is well suited for heavyweight management. Service management is still a fairly new area, and it seems that here the architecture of choice could be TINA, built using CORBA-based platforms. However, existing investment in network element management and network management realized with SNMP and TMN/OSI would need to be maintained. All these technologies would need to be integrated. SNMP devices can already be managed via TMN/OSI management using proxy agents, and some similar arrangement would be required for the inclusion of TMN/OSI entities within a TINA architecture based on CORBA. This three-way tiered integration seems a likely scenario for the future management of CATV digital networks and services.

A major stumbling block for all of these technologies is security. There is no overall security architecture for supporting integrated network and service management. At the time of writing, the security specifications for SNMPv3 exist, there is a specification for secure transactions for CORBA, TMN security standards look likely to be ratified soon, while security issues in TINA seem unclear. The provision of a secure service and management infrastructure is vital to allow the kind of dynamic online real-time buying and selling of services the CATV community perceives as vital to the uptake of the new digital services it hopes to offer in the future.

There are significant differences between the North American and European networks, especially when considering the return path. Many North American networks still rely on a telco return, whereas most European networks have broadband return-path capability. However, there are many common issues concerning the management of network elements, networks, and services. Europe looks set to use existing SNMP infrastructure accessible via OSI-SNMP proxies within a TMN framework to offer network element and network management. Service management will be via functions integrated into applications using CORBA/TINA. However, Europe lacks a single body for the CATV community that can act as a vehicle for promoting the adoption of standards. The North American CATV community has US CableLabs to help coordinate technical initiatives, and seems keen to follow the SNMP route at the moment.

Acknowledgments

The authors would like to thank the IBCoBN WG9 participants for their discussions, especially Richard Catchpole (Nortel, United Kingdom) for discussions on activities within IEEE802.14, DAVIC, and DVB; Pol Descamps (BARCO, Belgium) for discussions on fault detection within the CATV network; and Guy Ramlot (Integan, Belgium) for discussions on ingress noise.

The authors are grateful to the anonymous reviewers for their useful comments.

References

[1] IETF IPCDN WG, work in progress, Mar./May 1998.
[2] *IEEE Commun. Mag.*, vol. 35, no. 6, June 1997.
[3] *IEEE Network*, vol. 11, no. 1, Jan/Feb 1997.
[4] ITU Rec. G.774, "Synchronous Digital Hierarchy (SDH) Management Information Model for the Network Element View," Sept. 1992.
[5] http://www.atmforum.com/atmforum/specs/approved.html
[6] M. Ahmed and K. Tesink, Eds., "Definitions of Managed Objects for ATM Management Version 8.0 using SMIv2," RFC1659 Aug. 1994.
[7] ITU Rec. I.751, "Asynchronous Transfer Mode (ATM) Management of the Network Element View," work in progress, 1996.
[8] *IEEE Commun. Mag.*, vol. 35, no. 10, Oct. 1997.
[9] J. Case, C. Davin, and M. Fedor, "Simple Network Management Protocol — SNMP," RFC 1098, Apr. 1 1989.
[10] J. Case, K. McCloghrie, M. Rose, and S. Waldbusser, "Protocol Operations for Version 2 of the Simple Network Management Protocol (SNMPv2)," RFC 1905, Jan. 22, 1996.
[11] D. Levi, P. Meyer, and B. Stewart, "SNMPv3 Applications," RFC2263, Jan. 1998.
[12] ITU Rec. X.700, "Management Framework for Open systems Interconnection (OSI) for CCITT Applications," Sept. 1992.
[13] ITU Rec. M.3010, "Principles for a Telecommunications Management Network," Oct. 1992.
[14] M. T. Rose, and D. E. Cass, "ISO transport services on top of the TCP: Version 3." RFC1006, May 1 1987.
[15] TINA-C, "Overall Concepts and Principles of TINA," Feb. 1995.
[16] OMG, "Common Object Request Broker: Architecture and Specification," rev. 2.0 (OMG CORBA 2.0), July 1995.
[17] M. Laubach, "Using ATM over Hybrid Fiber-Coax Networks," presented at SPIE Eastern Conf., Philadelphia, PA, Oct. 23, 1995.
[18] B. Ellington, "LAN Emulation over ATM, Version 1.0," ATM Forum, 1995.
[19] A. Jones, I. Gurantz, and M. Maslaney, "ATM in MPEG-2 Transport — or Vice Versa," *Proc. 1996 Conf. Emerging Technologies*, San Francisco, CA, Jan. 8–10, 1996, pp. 231–40.
[20] ITU Rec. Q.2931, "Broadband Integrated Services Digital Network (B-ISDN) — Digital Subscriber Signaling System No. 2 (DSS 2) — User-Network Interface (UNI) Layer 3 Specification for Basic Call/Connection Ccontrol," Feb. 1995.
[21] R. Braden, "Resource ReSerVation Protocol (RSVP) — Version 1 Functional Specification," RFC2205, L. Zhang *et al.*, Eds., Sept. 1997.
[22] L. Degrossi and L. Berger, "Internet Stream Protocol Version 2 (ST-2) Protocol Specification — Version ST2+," RFC1819, Aug. 1995.
[23] *IEEE Commun. Mag.*, vol. 36, no. 3, Mar. 1998.
[24] DAVIC 1.0 Spec. Pt. 7, "High and Mid Layer Protocols," Geneva, Switzerland, 1995.
[25] DAVIC 1.0 Spec. Pt. 1, "Description of DAVIC Functionalities," Geneva, Switzerland, 1995–1997.
[26] G. Pavlou, K. McCarthy, S. N. Bhatti, and J. N. DeSouza, "Exploiting the Power of OSI Management for the Control of SNMP-Capable Resources Using Generic Application Level Gateways," *Proc. 4th ISINM*, Santa Barbara, CA, A. S. Sethi, Y. Raynaud, and F. Faure-Vincent, Eds., May 1–5, 1995, Chapman & Hall, pp. 440–53.
[27] TINA-C, "Management Architecture v2.0," Dec. 1994.
[28] ITU Rec. X.722, "Structure of Management Information; Guidelines for the Definition of Managed Object," Jan. 1992.
[29] X/Open and NMF, "Inter-Domain Management Specifications: Specification Translation," X/Open prelim. spec., work in progress, 1996.
[30] R. Atkinson, "Security Architecture for the Internet Protocol," RFC1825, Aug. 1995.
[31] S. N. Bhatti *et al.*, "Secure Remote Management," *Proc. 4th Int'l. Conf. Info. Network Sys. Mgmt.*, May 1–5, 1995, Santa Barbara, CA, A. S. Sethi, Y. Raynaud, and F. Faure-Vincent, Eds., Chapman & Hall, pp.156–69.
[32] S. N. Bhatti *et al.*, "Secure Management Information Exchange," *J. Network and Sys. Mgmt.*, vol. 4. no. 3, Sept. 1996.

Biographies

SALEEM N. BHATTI [M] (S.Bhatti@cs.ucl.ac.uk) holds a B.Eng in electrical and electronic engineering, an M.Sc in data communication networks and distributed systems, and a Ph.D. in computer science, all from University College London (UCL). Since October 1991 he has been a member of the research staff at UCL, and has recently been appointed as a lecturer in data communications and networking within the department. He has been involved in post-graduate teaching as well as various consultancy roles within industry. At UCL he has worked on various computer communication and networking related projects, covering topics such as network and systems management, network security, ISDN, ATM, QoS, multiservice networks, and residential broadband services. Saleem is a member of the ACM.

GRAHAM KNIGHT (G.Knight@cs.ucl.ac.uk) graduated in mathematics from the University of Southampton in 1969. He taught math and computer science in schools and colleges until 1979, when he obtained an M.Sc. in computer science from University College London. Since then he has worked at the college, initially as a research assistant, now as a senior lecturer. His research work has been in the field of computer communications. He has led UCL teams in ESPRIT projects concerning OSI, network management, and ISDN, and is now involved in a European ACTS program. Currently his research interests include routing in hybrid SDH/ATM networks, CATV-based Internet access, and the use of Java and the Web for network and systems management.