ISO/IEC JTC 1/SC 25/WG 1 N 1140a
Date: 2005-03-09

ISO/IEC JTC 1/SC 25 INTERCONNECTION OF INFORMATION TECHNOLOGY EQUIPMENT Secretariat: Germany (DIN)

DOC TYPE:	**2nd CD**
TITLE:	**ISO/IEC CD 20587 Information technology — Interconnection of information technology equipment — Home Electronic System — (HES) Gateway — A Broadband Home Network for the Home Electronic System (HES) (updated from N 1140)**
SOURCE:	**United States**
PROJECT:	**25.01.09**
STATUS:	**Working Draft of CD with comments on WG 1/N 694 resolved per WG 1/N 1005**
ACTION ID:	**ACT**
DUE DATE:	**N/A**
REQUESTED ACTION	**For discussion at WG 1 meeting in March 2005**
DISTRIBUTION:	**ISO/IEC JTC 1 SC 25 WG 1**

TABLE OF CONTENTS

FIGURES

FOREWORD

ISO (the International Organisation for Standardisation) and IEC (the International Electrotechnical Commission) form the specialised system for world-wide standardisation. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organisation to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organisations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work.

In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1. International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

ISO/IEC 20587 was prepared by Joint Technical Committee ISO/IEC JTC 1, Information technology, Subcommittee SC 25, Interconnection of Information Technology Equipment.

This standard is based on CEA-851 and CEA-851-A, which were developed by the Consumer Electronics Association (CEA). Work on CEA-851 was started by the Video Electronics Standards Association (VESA) in 1995 to create the architecture for a digital broadband home network. In January 2000 the Board of Directors of VESA and the Board of Directors of the Consumer Electronics Association agreed to merge this project into the CEA R7 Home Networking Standards Committee.

CEA-851, the Versatile Home Network, was issued as a standard in 2000. In 2004 CEA asked the 1394 Trade Association (1394TA) to help develop CEA-851-A by updating CEA-851 and accommodating UPnP™. The 1394TA presented a proposal for CEA-851-A to CEA in January 2005. The CEA Home Networking Committee approved CEA-851-A on March 8, 2005 for publication as an American National Standard. This document is being furnished to WG 1 by the CEA per agreement to assist with the development of ISO/IEC 20587.

INTRODUCTION

This standard defines an IP-enabled network for connecting cluster networks to a whole-home broadband distribution backbone in order to facilitate integrated operation of appliances and networked components. The distribution network in this standard is based on IEEE 1394. This network will accommodate Ethernet as an attached network via a bridge, and directly with the introduction of IEEE 1394c. The network defined in this standard is called the Versatile Home Network (VHN Home Network). The VHN Home Network provides a flexible and open network architecture and communications protocol specification for digital devices in the home.

Function and use of a VHN Home Network:

- Allows the transfer of information among all connected digital devices in the home, either as directly connected end devices or as part of a cluster network.
- Allows interoperability between devices on different cluster networks in the home, including low bandwidth networks and high bandwidth networks.
- Provides a common interface to Residential Gateways that connect devices in the home to access networks.
- Provides user-to-device control.
- Provides device-to-device control.
- Provides home network management for devices and applications.

NOTE: This standard defines a home intranet as a collection of networks that provides complete connectivity between end devices. This intranet uses the facilities of the TCP/IP protocol suite for asynchronous (and some isochronous) communications. Almost all of the underlying technologies, from media to applications, are defined elsewhere, as standards that were developed by national standards bodies, by international standards bodies, or by industry consortia. This standard is different from most other standards in that it places unusual emphasis on incorporation of these other technologies and protocols. In many cases, the entire technology or protocol is included by reference in this standard. Thus, a single sentence in this standard may imply hundreds of pages of definitions and requirements from other documents. It is important for the reader and user of this standard to understand that the underlying specifications must be respected, and carefully followed, for the VHN to be an effective integrating tool for the home network.

A Broadband Home Network for HES

VHN (Versatile Home Network)

1 Scope and Purpose

1.1 Purpose

The VHN enables several important classes of applications for the home network:

- **Entertainment services —** which include distribution of video, audio, and video games; and control of audio/video (A/V) devices such as TVs, VCRs, and set-top boxes.
- **Communication services —** which include voice telephony (wired and wireless), video telephony, video conferencing, distance learning, and remote access to corporate networks.
- **Information services —** which include Internet access, on-line service access, PC file and printer sharing, news and information on demand, home shopping, and home banking.
- **Home automation services —** which include lighting, appliance control, energy management, comfort control, and premises security.

Figure 1 shows a VHN Home Network that supports these services.

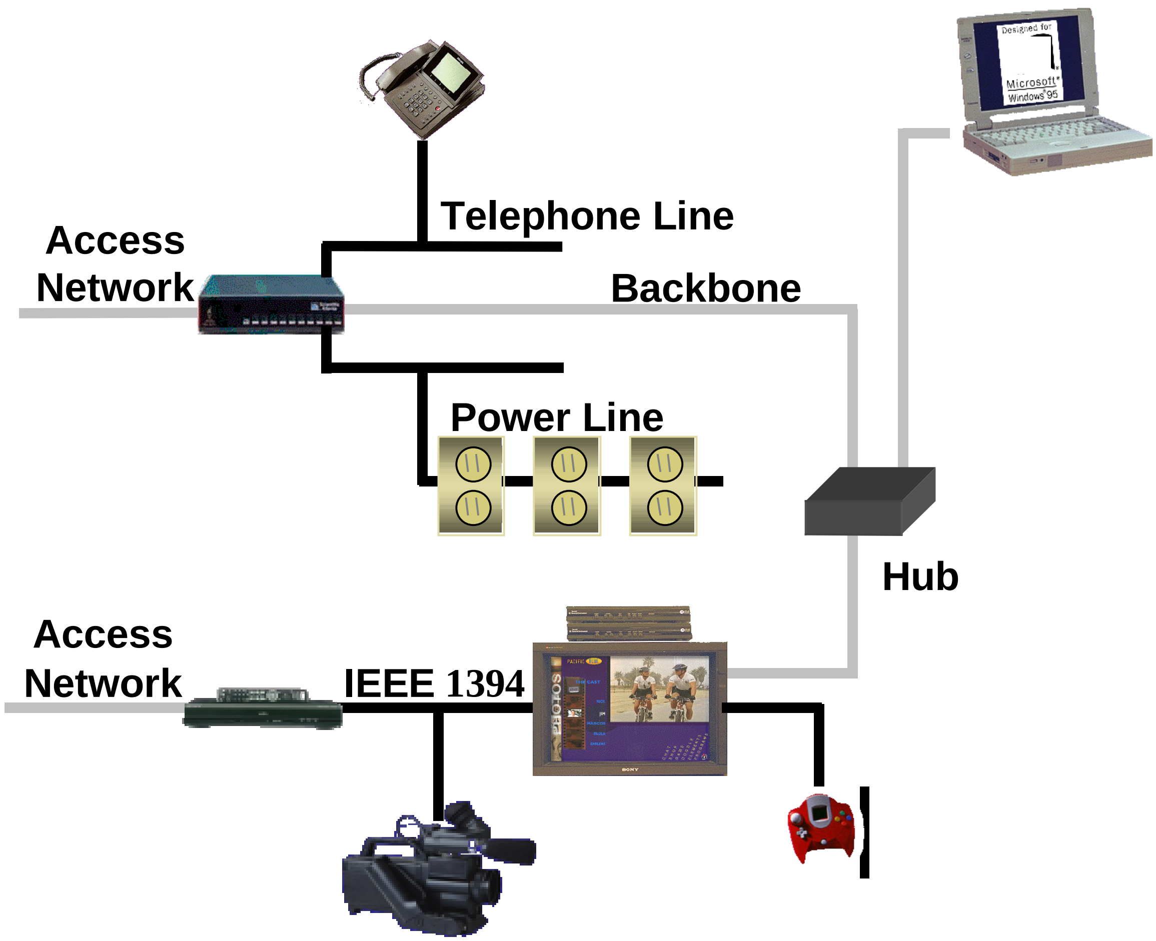


Figure 1 – A VHN Home Network

1.2 Scope

The VHN Home Network is defined by an abstract model (see Figure 2) that satisfies the needs of the classes of applications described in the Section 1.1. The model consists of:

- A backbone network.
- One or more component networks.
- A number of access devices that connect the home network to external access networks.
- A number of network devices that connect component networks to the home backbone network.
- End devices that provide various functional services to the home user.

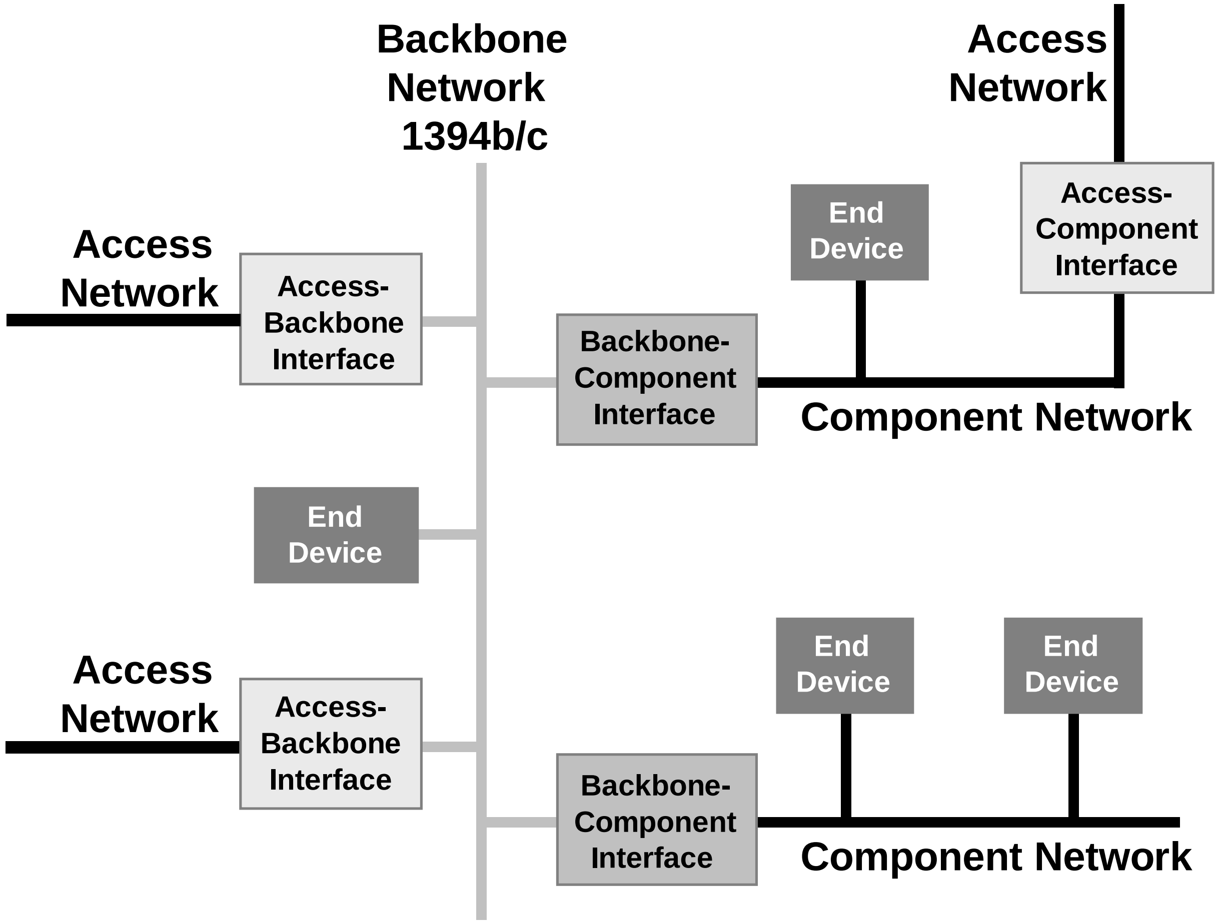


Figure 2 – An Abstract VHN Home Network

The key components of the VHN network architecture are:

- **End Device** — An end device is a digital device connected to the home network that provides some utility (other than network service) to the end user. Examples of end devices are printers, televisions, audio speakers, security sensors, and HVAC (Heating, Ventilating, and Air-Conditioning) controllers.

- **Component Networks** — The component networks enable the several devices connected to them to communicate with each other. The component network is connected to the backbone through a backbone-component interface. The choice of a component network for a particular device is dictated by the communication needs and cost points of the device. Some examples of important component networks are IEEE 1394-1995, Ethernet, HomePNA, X-10™, Powerline CEBus™, Echonet™, and RF Wireless LAN.

- **Backbone-Component Interface** — In VHN Home Network terminology, a network interconnection, or backbone-component interface device is an element that provides network services to end devices. Examples of network devices include repeaters, bridges, routers, brouters, and network management stations, or any device that implements such a function (e.g., a personal computer).

- **Access-Backbone Interface and Access-Component Interface—**An access-backbone interface connects an external access network to the home network. Access-component interfaces connect to a component interface through which a connection is made to the home network backbone. Some examples of access interfaces are a POTS modem, an xDSL adapter, a cable modem, a DBS (satellite TV service) decoder, and a Residential Gateway. ISO/IEC 15045, "Residential Gateway," defines a standard residential gateway that is referenced in this standard (see Section 8.1).

The VHN Home Network architecture is extremely flexible, allowing it to be adapted to meet the needs of many living styles. Annex A contains illustrations of three VHN Home Network implementations as examples of how the abstract architecture of Figure 2 may be translated into an actual VHN Home Network.

2 Normative References

2.1 Normative Reference List

The following standards contain provisions that, through reference in this text, constitute normative provisions of this standard. At the time of publication, the editions indicated were valid. All standards are subject to revision, and parties to agreements based on this standard are encouraged to investigate the possibility of applying the most recent editions of the standards listed in this section.

1. ANSI/CEA-2027-A, A User Interface for Home Networks Using Web-based Protocols, March 2005.

2. AV/C Digital Interface Command Set General Specification Version 4.2, http://www.1394ta.org.

3. Enhancements to the AV/C General Specification 3.0 Version 1.1, http://www.1394ta.org.

4. CEA-851.1, IP-Based Digital Telephony for the Versatile Home Network

5. CEA-851.2, Security Services for the Versatile Home Network

6. CEA-2007, QoS Priority Groupings for 802.1Q

7. IEEE 1394-1995 – Standard for a High Performance Serial Bus – Firewire, http://www.ieee.org

8. IEEE 1394.1-2004 – High Performance Serial Bus Bridges, http://www.ieee.org

9. IEEE 1394a-2000 – IEEE Standard for a High Performance Serial Bus- Amendment 1, http://www.ieee.org

10. IEEE 1394b-2002 – IEEE Standard for a Higher Performance Serial Bus-Amendment 2, http://www.ieee.org

11. IEEE p1394c-200x – IEEE Standard for a Higher Performance Serial Bus-Amendment 3, draft 0.3, April 27, 2004, http://grouper.ieee.org/groups/1394/c/1394c.pdf

12. IEC 61883-1 – Consumer Audio/Video Equipment – Digital Interface, 1998.

13. IP1394, IPv4 over IEEE 1394, P. Johansson, September 1998, ftp://ftp.ietf.org/internet-drafts/draft-ietf-ip1394-ipv4-11.txt.

14. ISO 639, ISO-639: Code for the representation of names of languages, 1988 et seq. http://www.iso.ch. (ISO is the International Organization for Standardization.)

15. IEEE 802.1d, Annex H (formerly 802.1p), ISO/IEC 15802-3:1998, *IEEE Standard for* Information *technology--Telecommunications and information exchange between systems–IEEE standard for local and metropolitan area networks--Common specifications--Media access control (MAC) Bridges,* IEEE 802.1D, 1998 Edition.

16. IEEE 802.1q, IEEE Standard for Local and Metropolitan area networks: Virtual Bridged Local Area Networks, IEEE, December 1998.

17. ISO 8601, ISO, ISO 8601:1988 (E), Data elements and interchange formats - Information interchange - Representation of dates and times, 1998. http://www.iso.ch

18. ISO/IEC 10646, ISO/IEC 10646-1993 (E). Information technology – Universal Multiple-Octet Coded Character Set (UCS) -- Part 1: Architecture and Basic Multilingual Plane. [Geneva]: International Organization for Standardization, 1993 (plus amendments AM 1 through AM 7). http://global.ihs.com or http://www.iso.ch

19. ISO/IEC 15018 Information technology — Interconnection of information technology equipment — Generic cabling for homes. http://www.iso.ch

20. ISO/IEC 15045-1 Information technology — Interconnection of information technology equipment — Home Electronic System [HES] — Part1: A Residential gateway model for HES. http://www.iso.ch

21. OG-UUID, The Open Group, Universal Unique Identifier Format

22. OTP, The Open Trading Protocol Consortium. Internet Open Trading Protocol Part 2: Specification. Version 0.9, 12 January 1998., http://www.otp.org

23. RFC 1945, T. Berners-Lee, R. Fielding, H. Frystyk, Hypertext Transfer Protocol - HTTP/1.0

24. RFC1738, "Uniform Resource Locators", T. Berners-Lee, L. Masinter, and M. McCahill, December 1994. Available at ftp://ftp.isi.edu/in-notes/rfc1738.txt.

25. RFC-1766, H. Alvestrand. March 1995, Tags for the Identification of Languages

26. RFC1808, "Relative Uniform Resource Locators", R. Fielding, June 1995. Available at ftp://ftp.isi.edu/in-notes/rfc1808.txt.

27. RFC-2045**,** N. Freed & N. Borenstein. November 1996, *Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies.*

28. RFC-2046**,** N. Freed & N. Borenstein. November 1996, *Multipurpose Internet Mail Extensions (MIME) Part Two: Media Types.*

29. RFC-2311**,** Dusse, S., P. Hoffman, B. Ramsdell, L. Lundblade, and L. Repka. *S/MIME Version 2 Message Specification* [RFC 2311]. March 1998.

30. RFC-959, J. Postel, J. Reynolds, *File Transfer Protocol*

31. SSL**,** Freier, Alan O., Philip Karlton, and Paul C. Kocher. *The SSL Protocol Version 3.0* [http://www.netscape.com/eng/ssl3/ssl-toc.html]. Netscape Communications Corporation: March 1996. As amended by SSL 3.0 Errata of August 26, 1996 [http://www.netscape.com/eng/ssl3/ssl-errata.html].

32. TIA-570-B Residential Telecommunications Infrastructure Standard (ANSI/TIA-570-B-2004).

33. UPnP AV Architecture:0.83 for UPnP™ Version 1.0, Preliminary Design, June 12, 2002

34. UPnP AVTransport for UPnP™ Version 1.0, Preliminary Design, June 25, 2002

35. UPnP ConnectionManager:1 Service Template Version 1.01 for UPnP™ Version 1.0, June 25, 2002.

36. UPnP ContentDirectory:1 Service Template Version 1.01 for UPnP™ Version 1.0, June 25, 2002.

37. UPnP™ Device Architecture, Version 1.0, June 2000 http://www.upnp.org.

38. UPnP Device Architecture, Annex A–IPv6, August 8, 2002.

39. UPnP InternetGatewayDevice:1 Device Template Version 1.01 for UPnP™ Version 1.0, November 12, 2001.

40. UPnP MediaServer:1 Device Template Version 1.01 for UPnP™ Version 1.0, June 25, 2002.

41. UPnP MediaRenderer:1 Device Template Version 1.01 for UPnP™ Version 1.0, June 25, 2002.

42. W3C-NOTE-datetime**,** Misha Wolf, Charles Wicksteed, Date and Time Formats http://www.w3c.org

43. XML-NS, "Namespaces in XML", 27th March 1998, W3C Working Draft (http://www.w3.org/TR/WD-xml-names)

2.2 Request For Comments (RFCs)

The following Requests For Comment filings are referenced in this standard:

RFC 879	The TCP Maximum Segment Size and Related Topics
RFC 815	IP Datagram Reassembly Algorithms
RFC 813	Window and Acknowledgment Strategy in TCP/IP
RFC 793	(MIL STD 1778) Transmission Control Protocol (TCP)
RFC 792	Internet Control Message Protocol (ICMP)
RFC 791	(MIL STD 1777) Internetwork Protocol (IP)
RFC 768	User Datagram Protocol (UDP)
RFC 1918	Address Allocation for Private Internets – specifies IANA private network addresses - and their uses
RFC 1631	The IP Network Address Translator (NAT) - How to make the private home network access the internet
RFC 1531	Dynamic Host Configuration Protocol, Easy IP – Sections as appropriate for the role of the device.
RFC 1112	Host Extensions for IP Multicasting
RFC 1101	DNS Encoding of Network Names and Other Types
RFC 1035	Domain Names---Implementation and Specification
RFC 1034	Domain Names---Concepts and Facilities
RFC 1889	RTP: A Transport Protocol for Real-Time Applications
RFC 2131	Dynamic Host Configuration Protocol
RFC 2326	Real Time Streaming Protocol (RTSP)
RFC 2616	HTTP v1.1
RFC 3066	Tags for the Identification of Languages
Draft-IETF-IP1394-IPv4	IPv4 over 1394 – or corresponding RFC when ratified.
Draft-gentric-avt-rtsp-http-00	Gentric – or corresponding RFC when ratified

2.3 Informative References

1. DES, National Institute of Standards and Technology, U.S. Department of Commerce. Data Encryption Standard [NIST FIPS PUB 46-1], January 1988.

2. DH, American National Standards Institute. Accredited Standards Committee X9 Working Draft: American National Standard X9.42-1993: Public Key Cryptography for the Financial Services Industry: Management of Symmetric Algorithm Keys Using Diffie-Hellman. American Bankers Association, September 21, 1994.

3. DSS, National Institute of Standards and Technology, U.S. Department of Commerce. Digital Signature Standard [NIST FIPS PUB 186]. 18 May 1994.

4. PKCS-1, RSA Laboratories. PKCS #1: RSA Encryption Standard. Version 1.5, November 1993.

5. PKCS-7, RSA Laboratories. PKCS #7: Cryptographic Message Syntax Standard. Version 1.5, November 1993.

6. RFC-2119, S. Bradner, Key words for use in RFCs to Indicate Requirement Level

7. RFC-2268, Rivest, R. A Description of the RC2® Encryption Algorithm [RFC 2268]. March 1998.

8. TLS, Dierks, Tim and Christopher Allen. The TLS Protocol Version 1.0. Work in progress.

9. XMLCIM-WP, “XML as a Representation for Management Information - A White Paper", Roger Booth, Microsoft Corporation, 1998 (http://wbem.freerange.com/wbem/xml_whitepaper.doc)

3 Definitions and Abbreviations

3.1 Definitions

The following terms are used in this standard and commonly used in other industry publications. As used in this standard, they have the following meanings:

Access Line	A facility that connects the home to an external access network.
Access Network	A network external to the home.
Address	A sequence of characters that uniquely identify a network destination (endpoint) in a communication system.
ADSL	Asymmetric Digital Subscriber Line, a high-bandwidth access technology that uses the in-place copper loop. Bitrate is “asymmetric” in the directions to and from the home: To the home, bitrate may be between 1.544 Mb/s and 8.448 Mb/s (depending on the distance from the access provider’s termination), while bitrate from the home may be between 16 kb/s and 640 kb/s (again, depending on distance).
Aggregation	A strong form of an *association*. For example, the containment relationship between a system and the components that make up the system can be called an *aggregation*. An *aggregation* is expressed as a *Qualifier* on the *association* class. *Aggregation* often implies, but does not require, that the aggregated *objects* have mutual dependencies.
Association	A *class* that expresses the relationship between two other *classes*. The relationship is established by the presence of two or more *references* in the *association class* pointing to the related *classes*.

Asynchronous Transmission	Data transmission between devices that are not synchronized with one another using a clocking mechanism or other technique.
AV/C	The Audio/Video Control language developed by the IEEE 1394 Trade Association used to control consumer audio/video equipment.
Bandwidth	The range of frequencies occupied by a signal
Bridging	Connecting two or more network segments or subnetworks at the Data Link layer of the OSI Reference Model.
Browser	A Presentation Engine that is capable of rendering HTML documents on a display.
CAL	The Common Application Language, developed as the control language for CEBus.
Cardinality	A relationship between two classes that allows more than one *object* to be related to a single *object*. For example, Microsoft Office™ is made up of the software elements Word, Excel, Access and PowerPoint.
Catalog	A set of service offers. A Client obtains a catalog from a Server, and uses the offers within the catalog to locate a service.
CEBus	The Consumer Electronics Bus, an EIA standard for home data networking on twisted pair, coax, powerline and IR; CEBus uses the CAL language for control.
CIM	Common Information Model is the schema of the overall managed environment. It is divided into a *Core model*, *Common model* and *extended schemas*.
CIM Schema	The schema representing the *Core* and *Common models*. Versions of this schema will be released by the DMTF over time as the schema evolves.
Class	A collection of instances, all of which support a common type; that is, a set of *properties* and *methods*. The common *properties* and *methods* are defined as *features* of the *class*. For example, the *class* called Modem represents all the modems present in a system.
Client	One of the two parties in a VHNE relationship (the other one being the Servers). The Client uses VHNE to obtain information and control/management information from the Servers.
Common model	A collection of *models* specific to a particular area, derived from the *Core model*. Included are the system *model*, the application *model*, the network *model* and the device *model*.
Conditional Access	The strategy and process that denies access to services based on authorization or payment.
Control	The vertical plane, or stack, in the network protocol model, which contains all of the protocol layers that are specifically dedicated to providing control and signaling. Control function can be from user to devices (user-to-device control), or between devices (device-to-device control).
Core model	A subset of *CIM*, not specific to any platform. The *Core model* is

	set of *classes* and *associations* that establish a conceptual framework for the *schema* of the rest of the managed environment. Systems, applications, networks and related information are modeled as extensions to the *Core model*.
Device Discovery	The action that determines the existence and attributes of devices in a network system. Action may be either automatically or manually initiated.
Domain	A virtual room for object names that establishes the range in which the names of objects are unique.
End Device	An end device is a digital device in the home whose purpose is to provide some benefit (other than network service) to the end user.
Ethernet	A network technology defined by the IEEE 802.3 specification.
Explicit Qualifier	A *qualifier* defined separately from the definition of a *class*, *property* or other schema element (see i*mplicit qualifier*). *Explicit qualifier* names must be unique across the entire *schema*. *Implicit qualifier* names must be unique within the defining schema element; that is, a given schema element may not have two *qualifiers* with the same name.
Extended schema	A platform specific *schema* derived from the Common model. An example is the Win32 *schema*.
Feature	A *property* or *method* belonging to a *class*.
Firewall	A device that is inserted between the premises network and the access line to establish a controlled link and to erect an outer security wall or perimeter to protect the premises network from access line-based attacks and to provide a single choke point where security and audit can be imposed.
FireWire™	The Apple trademarked name for the IEEE 1394 high-performance serial bus.
Flavor	Part of a *qualifier* specification indicating overriding and *inheritance* rules. For example, the *qualifier* KEY has Flavor(DisableOverride ToSubclass), meaning that every subclass must inherit it and cannot override it.
Gateway	A device that serves as a point of entry, generally from a local network to a larger network; gateways may interface the networks at all seven layers of the OSI Reference Model.
Generic CAL	An expansion and enhancement of the CAL language that allows CAL to be used in home networks that are not based on CEBus.
Home Network	An in-home network, usually digital, that implements communication between end devices in the home, and between end devices and devices external to the home through access lines.
IEEE 1394	A high performance serial bus that provides both isochronous and asynchronous connectivity between devices.
Implicit Qualifier	A *qualifier* defined as a part of the definition of a *class*, *property* or other schema element (see *explicit qualifier*).
Indication	A type of *class* usually created as a result of the occurrence of a

	trigger.
Inheritance	A relationship between two *classes* in which all the members of the *subclass* are required to be members of the *superclass*. Any member of the *subclass* must also support any *method* or *property* supported by the *superclass*. For example, Modem is a *subclass* of Device.
Instance	A unit of data. An *instance* is a set of *property* values that can be uniquely identified by a *key*.
ISO	The International Organization for Standardization, a worldwide federation of national standards bodies.
Isochronous transmission	Data transmission in which the time between the arrival of contiguous data packets is closely matched to time between their transmission, an important attribute of streaming data such as audio and video.
Key	One or more qualified class properties that can be used to construct a name. One or more qualified object properties which uniquely identify instances of this object in a namespace.
Managed Object	The actual item in the system environment that is accessed by the *provider*. For example, a Network Interface Card.
Message	The abstract concept of an atomic unit of communication. In this specification, the term *message* does not denote any specific protocol structure; rather, it is used to denote an abstract communication concept.
Meta model	A set of *classes*, *associations* and *properties* that expresses the types of things that can be defined in a *Schema*. For example, the *meta model* includes a *class* called property which defines the *properties* known to the system, a *class* called method which defines the *methods* known to the system, and a *class* called class which defines the *classes* known to the system.
Meta schema	The schema of the meta model.
Method	A declaration of a signature; that is, the method name, return type and parameters, and, in the case of a concrete class, may imply an implementation.
Minimal Client	A Client VHNE implementation that has no persistent server component and therefore cannot receive messages from a Servers.
Model	A set of *classes*, *properties* and *associations* that allows the expression of information about a specific domain. For example, a Network may consist of Network Devices and Logical Networks. The Network Devices may have attachment *associations* to each other, and may have member *associations* to Logical Networks.
Model Path	A reference to an object within a namespace.
MPEG-2	A digital video compression standard developed by the Moving Picture Experts Group.
Name	Combination of a Namespace path and a Model path that identifies a unique object.

Namespace	An *object* that defines a scope within which object keys must be unique.
Namespath Path	A reference to a namespace within an implementation that is capable of hosting CIM objects.
Network Management	The operation or system that is responsible for managing a network (or a portion of the network) providing access to a wide variety of information regarding network configuration, performance and status.
Network Protocol	A link-layer independent protocol at level 3 of the 7-layer OSI Reference Model that allows devices on diverse link-layer networks to communicate with each other.
OSI Reference Model	The Open Systems Interconnection Reference Model, developed by ISO, that defines a layered architecture in which each of seven layers performs specified tasks that are used by the layer above to effect communication between devices.
Payload	A protocol structure encapsulating a set of logical VHNE operations delivered at discrete intervals. A *payload* is a single instance of an XML document formatted according to the protocol definitions contained in this specification.
Polymorphism	A *subclass* may redefine the implementation of a *method* or *property* inherited from the associated *superclass*. The *property* or *method* is thereby redefined, even if the *superclass* is used to access the object. For example, Device may define availability as a string, and may return the values “powersave,” “on” or “off.” The Modem *subclass* of Device may redefine (override) availability by returning “on,” “off,” but not “powersave.” If all Devices are enumerated, any Device that happens to be a modem will not return the value “powersave” for the availability *property*.
POTS	Plain Old Telephone Service, analog voiceband telephone service.
Property	A value used to characterize an instance of a *class*. For example, a Device may have a *property* called status.
Provider	An executable that can return or set information about a given *managed object*.
Qualifier	A value used to characterize a *method*, *property*, or *class* in the *meta schema*. For example, if a property has the qualifier KEY with the value TRUE, the property is a key for the class.
Receiver	Generic term referring to the target of an VHNE payload. The term Receiver is used when it is possible for either the Client or the Servers to be the party receiving the payload.
Reference	Special *property types* that are references or “pointers” to other instances.
Request	A message asking for the performance of an operation. Requests in VHNE are messages carried by payloads.
Requestor	Generic term referring to the initiator of an VHNE payload

	request.
Residential Gateway	A device that mediates between one or more access network technologies and one or more home network technologies.
Responder	Generic term referring to the recipient of an VHNE payload request.
Response	A message containing the results of an operation. Responses in VHNE are messages carried by payloads.
Routing	The process of directing information towards their ultimate and intended destination based on a knowledge of the network topology, the network-addressing scheme and in some cases of network traffic levels. In connection oriented networks this involves the process of selecting a connection path at the time of connection-oriented environments.
Schema	A namespace and unit of ownership for a set of classes. *Schemas* may come in forms such as a text file, information in a repository, or diagrams in a CASE tool.
Scope	Part of a *Qualifier* specification indicating with which meta constructs the *Qualifier* can be used. For example, the *Qualifier* ABSTRACT has Scope (Class Association Indication), meaning that it can only be used with *Classes*, *Associations* and *Indications*.
Scoping Object	Objects which represent a real-world managed element, which in turn propagate keys to other objects.
Sender	Generic term referring to the originator of a VHNE payload. The term Sender is used when it is possible for either the Client or the Servers to be the party sending the payload.
Servers	One of the two parties in a VHNE relationship (the other one being the Client). The Servers uses VHNE to send information and control/management information to the Client.
Service	An definition of 'interface' provided by a service and how to access it.. There may be many independent services between a Server and a Client.
Service Offer	A proposed set of parameters for a particular service.
Signature	The return type and parameters supported by a *method*.
Stream [OMG Definition]	A stream is a set of flows of data between objects, where a flow is a continuous sequence of frames in a clearly identified direction.
Stream Interface [OMG Definition]	A stream interface is an aggregation of one or more source and sink flow end-points associated with an object.
Subclass	See *Inheritance*.
Superclass	See *Inheritance*.
Top Level Object	A class or object that has no scoping object.
Transaction Security	The operation or process that ensures the integrity, i.e., completion, restart, rollback, and rollforward of a sequence of events related in a fixed chronological series of transactions on a networked system.
Trigger	The occurrence of some action such as the creation, modification

	or deletion of an *object*, access to an *object*, or modification or access to a *property*. *Triggers* may also be fired as a result of the passage of a specified period of time. A *trigger* typically results in an *Indication*.
Twist	In the context of fiber connections, the transposition of fibers at a connector, so that the "receive" fiber and the "transmit" fiber are correctly oriented.
Twisted Pair	A communication medium that uses two copper wires twisted hellically to reduce crosstalk and radio frequency emission and susceptibility.
UI	User Interface - the unit that handles the user's service selection
Unsolicited Message	A protocol mechanism used in VHNE to provide a way for a Server to initiate communication to a Minimal Client.
VHN Media Controller	A device that presents a VHN Media Player or VHN Media Server control functions and status information. It also acts as a control mechanism for media management, transport, and output settings of any VHN Media Player or VHN Media Server on an IP-based streaming network. VHN Media Controller complies with all requirements in the VHN specification for a VHN Media Controller.
VHN Media Device	A product that functions as a VHN Media Server, VHN Media Player, and/or VHN Media Controller on an IP-based streaming network.
VHN Media Player	A device that receives, decodes, and displays video, audio, and/or images, and complies with all requirements in the VHN specification for a VHN Media Player.
VHN Media Server	A device that transmits (and optionally captures, repurposes, and/or stores) video, audio, and/or images, and complies with all requirements in the VHN specification for a VHN Media Server.
VHN Network Router	A device that contains the functionality of an Ethernet router [IEEE802.1d, Annex H], and complies with all requirements in the VHN specification for a VHN Network Router on an IP-based streaming network.
VHNE	VHN Home Network Exchange.
VHNE/HTTP	The specific binding of the VHNE protocol to the HTTP protocol.

3.2 Abbreviations

The following acronyms and abbreviations are used in this standard and commonly used in other industry publications.

1394TA	1394 Trade Association
A/V	Audio/Video
ABI	Access-Backbone Interface
ACI	Access-Component Interface

ADSL	Asymmetric Digital Subscriber Line
ANSI	American National Standards Institute
API	Application Programming Interface
ATM	Asynchronous Transfer Mode
AV/C	Audio/Video Control
BCI	Backbone-Component Interface
CAL	Common Application Language
CATV	Community Access Television (cable television)
CE	Consumer Electronics
CEBus	Consumer Electronics Bus
CIM	Common Information Model
CORBA	Common Object Request Broker Architecture
CSR	Control and Status Registers
CSS1	Cascading Style Sheets, Level 1
CTS	Command/Transaction Set
D2D	Device-to-Device
DBS	Direct Broadcast Satellite
DER	Distinguished Encoding Rules
DES	Data Encryption Standard
DH	Diffie-Hellman (key exchange)
DHCP	Dynamic Host Configuration Protocol
DMTF	Distributed Management Task Force
DSA	Digital Signature Algorithm
DSLAM	Digital Subscriber Line Access Module
DSS	Direct Satellite Service
DTD	Document Type Definition
DTV	Digital Television
DVCR	Digital VCR
DVD	Digital Versatile (or Video) Disk
ECMA	European Computer Manufacturers Association
EIA	Electronic Industries Alliance
EST	Eastern Standard Time
FCP	Function Control Protocol
GIF	Graphics Interchange Format
GOF	Glass optical fiber
GUI	Graphical User Interface
HAVi	Home Audio/Video Interoperability
HDTV	High-Definition Television
HFC	Hybrid Fiber/Coax
HN	Home Network
HNB	Home Network Broker
HTML	Hypertext Markup Language
HTTP	Hypertext Transfer Protocol
HVAC	Heating, Ventilation, and Air Conditioning
IEC	International Electrotechnical Commission

IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IOTP	Internet Open Trading Protocol
IP	Internet Protocol
IPSEC	Internet Protocol Security
IPv4	IP version 4
IR	Interface Repository
ISDN	Integrated Services Digital Network
IV	Instance Variable
JPEG	Joint Photographic Experts Group
LAN	Local-area network
MAC	Medium Access Control
MD5	Message Digest 5
MIB	Management Information Base
MIME	Multipurpose Internet Mail Extensions
MPEG	Motion Picture Experts Group
NAT	Network Address Translation
OMG	Object Management Group
OSD	On-screen display
OSI	Open Systems Interconnection
OTR	One Touch Record
PC	Personal Computer
PCI	Protocol Control Information
PDU	Protocol Data Unit
PHY	Physical Layer
PKCS	Public Key Cryptography Standard
PNG	Portable Network Graphics
POF	Plastic optical fiber
POTS	Plain Old Telephone Service
QoS	Quality of Service
RC4	Rivest Cipher 4
RFC	Request for Comments
RG	Residential Gateway
ROM	Read-only memory
RPC	Remote Procedure Call
RSA	Rivest Shamir Aldeman
S/MIME	Secure Multipurpose Internet Mail Extensions
SDU	Service Data Unit
SHA	Secure Hash Algorithm
SSL	Secure Socket Layer
STB	Set-Top Box
TBD	To be determined
TCP	Transmission Control Protocol
TDR	Time Delayed Record
TIA	Telecommunications Industry Association

TLS	Transport Layer Security
TV	Television
UDP	User Data Protocol
UI	User Interface
UPnP	Universal Plug and Play
URL	Uniform Resource Locator
UTC	Universal Coordinated Time
UTF	Universal Text Format
UTP	Unshielded Twisted Pair
UUID	Universal Unique Identifier
VCR	Video Cassette Recorder
VHNE	VHN Home Network Exchange
WAN	Wide-area network
WBEM	Web-Based Enterprise Management
WWWUID	World-Wide Web Unique Identifier
XCE	Extensible Consumer Electronics
XDSL	x-Digital Subscriber Line ("x" may be A, H, S,V)
XML	Extensible Markup Language
XMLRPC	XML-based RPC
XSL	Extensible Stylesheet Language

4 Conformance

4.1 VHN Home Network

Sections 5 through 8 specify the VHN Home Network. All requirements listed in these sections shall be implemented for conformance with this standard.

4.2 VHN Devices

Three classes of VHN devices are described below. To be considered VHN compliant, each device must meet the criteria specified.

- **VHN Hub —** The VHN hub is located logically at the center of the star wiring configuration. This device shall conform to the media requirements as specified in Section 5.2 and physical layer requirements as specified in Section 5.3. The VHN hub may conform to the IEEE 1394.1-2004 standard for bridging in order to increase system bandwidth and minimize the propagation of bus resets.

- **VHN Backbone Device —** A VHN backbone device shall conform to the media requirements as specified in Section 5.2 and physical layer requirements as specified in Section 5.3. Additionally, these devices shall conform to the network layer services required in Section 5.5 and the user to device and device-to-device controls specified in Sections 6.2 and 6.3. IEC 61883 or other streaming technology may be used for A/V VHN backbone devices. VHN backbone devices may be end devices or interface devices.

- **VHN Device —** A VHN device shall conform to the network layer services required in Section 4 and the user-to-device and device-to-device controls specified in Sections 6.2 and 6.3. A VHN device is not required to support the VHN media. IEC 61883 or other streaming technology may be used for A/V VHN backbone devices. VHN devices may be end devices or interface devices.

End Devices not capable of talking to the VHN are not VHN-compliant. A non-VHN device may act as a VHN device by using a proxy service in an interface device.

Although the abstract architecture of the VHN Home Network classifies network elements as backbone networks, component networks, network devices, end devices, or access devices, this classification merely denotes the role of the element. In fact, a single physical device, such as a PC, may act simultaneously as an end device, an access device, and a network device.

As can be seen from Figure 2 the VHN Home Network may be composed of heterogeneous networks. There are several methods for connecting heterogeneous networks, including bridging, heterogeneous bridging, tunneling, and internetworking. VHN specifies IP as the internetworking protocol. Specifications for implementing IP on the VHN Home Network are included in Section 5.5 of this standard. IP enables a basic level of communication among all devices in the home. This ensures that any device in the home can exchange messages and data streams with any other device in the home, and can access any service available over the home network. Additionally, network devices that connect to the backbone network use the internetworking protocol to communicate among themselves.

5 Network Infrastructure

5.1 Overview of Media and Topology

The following sections contain requirements and specifications for media used and network topology to implement the whole-house “backbone” portion of a VHN Home Network.

Media and associated connectors shall consist of one or more of the following transmission technologies:

1. Unshielded twisted-pair (UTP) cabling

2. Glass optical fiber (GOF)

[Future issues of this standard may include the following option:

3. Plastic optical fiber (POF)]

Media forming the backbone component of the VHN Home Network shall be configured in a star topology.

Detailed specifications are presented in the following sections.

5.2 Physical Media

Media used for the backbone portion of the VHN Home Network shall conform to the specifications in this section.

5.2.1 Category 5e UTP

Category 5 Unshielded Twisted-Pair cable and connectors shall conform to the requirements for Category 5 UTP contained in ISO/IEC 15018 (see also TIA-570-B). In this standard all references to Category 5 shall be interpreted as Category 5e.

5.2.2 Glass Optical Fiber

Glass optical fiber (GOF) shall be 50/125-µm multimode fiber, and shall conform the requirements for such fiber contained in TIA-570-B. (Proposed amendments to ISO/IEC 15018 address GOF.)

Connectors used for GOF shall conform to requirements for optical fiber connectors in TIA-570-B.

5.2.3 Plastic Optical Fiber

[Future issues of this standard may include the following specifications*:*

Plastic optical fiber (POF) shall conform to the requirements for such fiber contained in IEEE 1394b. (Proposed amendments to ISO/IEC 15018 address POF.)

NOTE: POF *has distance limitations different from those for Category 5 UTP and GOF; see Section 5.4 below. POF shall be used only when the reduced length of the POF segment will be sufficient to reach the termination point from the center of the star.*

Connectors *used for POF shall conform to requirements for plastic optical fiber connectors in IEEE 1394b]*

5.3 Topology

An abstract view of a VHN Home Network is illustrated in Figure 2. Media forming the whole house backbone portion of the VHN Home Network shall be configured in a star topology. The “center” of the star shall be either an IEEE 1394 multiport repeater (i.e., a hub), or an IEEE 1394 bridge, as specified in Section 8.1 below.

The cable between the hub and outlet/connector shall not exceed 90 meters for Category 5 UTP or GOF. The 90-meter length allows an operational length of 100 meters including equipment and patch cords.

Each cable run from the hub to the outlet/connector shall follow the interconnection requirements of ISO/IEC 15018. A single, uninterrupted segment of medium (sometimes known as “home run”) is recommended between the hub and outlet.

*[*Future *issues of this standard may include the following specification:*

The cable between the hub and outlet/connector shall not exceed 50 meters for POF. The 50-meter length allows an operational length of 60 meters including equipment and patch cords.]

5.4 Backbone Physical & Data Link Layer (IEEE 1394b)

The physical and data-link layers shall conform to the relevant requirements specified in IEEE 1394-1995 as amended by IEEE 1394a-2000, IEEE 1394b-2002, and IEEE P1394c. A description of IEEE P1394c, under development by the IEEE to accommodate Ethernet, is provided in Annex B. Specific requirements for the media specified in this standard are as follows:

- The electrical signaling and media connections on Category 5 UTP media shall conform to the requirements specified in Clause 9 of IEEE 1394b-2002.
- The optical signaling and media connections on Glass Optical Fiber media shall conform to the requirements specified in Clause 7 of IEEE 1394b-2002.
- The optical signaling and media connections on Plastic Optical Fiber media shall conform to the requirements specified in Clause 8 of IEEE 1394b-2002.
- The configuration of connections on Category 5 UTP, Glass Optical Fiber and Plastic Optical Fiber media shall conform to the requirements specified in Clause 11 of IEEE 1394b-2002.
- The data and control signaling on Category 5 UTP, Glass Optical Fiber and Plastic Optical Fiber media shall conform to the requirements specified in Clause 10 of IEEE 1394b-2002.
- The arbitration and packet encoding on Category 5 UTP, Glass Optical Fiber and Plastic Optical Fiber media shall conform to the requirements specified in Clause 15 of IEEE 1394b-2002.

In addition to the requirements specified above, IEEE 1394b-2002 requires that a “twist” be included at some point in a connection between two 1394 nodes for fiber, but states that further specification is outside the scope of the standard. For fiber media, a twist shall be implemented at the center of the star on each of the connections on the hub or bridge placed at this location.

5.5 Protocol Stacks, Network Layers, Services & Streams

This section defines the protocol stacks required for the interconnection of various networks in a VHN Home Network. The parameters for each of the protocols are specified, as well as optional protocols where applicable. The VHN protocol stack is based on the OSI Reference Model for Communications, which is summarized in Annex C.

5.5.1 Protocol Stacks Overview

Protocol stacks for the VHN Home Network are shown in Figure 3. This complement of mandatory protocols is required only for VHN devices.

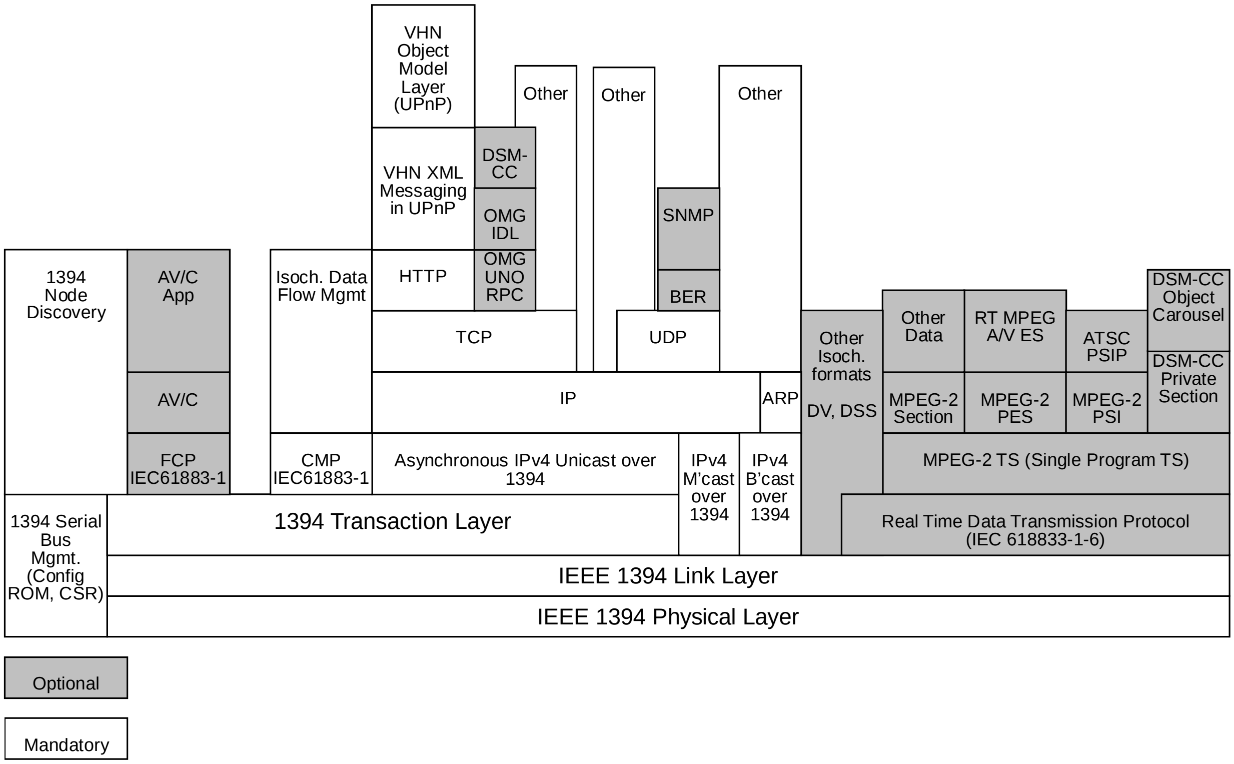


Figure 3 – VHN Protocol Stacks

5.5.2 IEEE 1394 Initialization

The protocol stack for IEEE 1394 Initialization is defined in Figure 4

<table>
<tr><td rowspan="3">IEEE 1394 Node Discovery Application</td><td>Unit or Subunit Identifier Descriptor Discovery Application (for AV/C devices)</td></tr>
<tr><td>AV/C Read Descriptor Command</td></tr>
<tr><td>Function Control Protocol – FCP (IEC61883-1) (for AV/C devices)</td></tr>
<tr><td rowspan="3">IEEE 1394 Serial Bus Management

(Configuration ROM, CSR)</td><td>IEEE 1394 Transaction Layer</td></tr>
<tr><td>IEEE 1394 Link Layer</td></tr>
<tr><td>IEEE 1394 Physical Layer</td></tr>
</table>

Figure 4 – Protocol Stack for Initialization

5.5.2.1 IEEE 1394 Node Discovery

The IEEE 1394 Node Discovery application shall be invoked after a bus reset event in the IEEE 1394 bus. IEEE 1394 Node discovery application will query all other devices on the IEEE 1394 bus to collect the information in the Configuration ROM of each device. This application will build a device information table that will, at minimum, correlate the node ID and WWUID (World Wide Web Unique ID) of every device on the bus. The use of smart bus scanning is encouraged to minimize the amount of bus traffic immediately following a bus reset.

5.5.2.2 AV/C Node Discovery

This procedure is used to discover nodes supporting AV/C. The Unit (or Subunit) Identifier Descriptor Discovery Application shall be invoked at the device power-up. It must be invoked at the bus-reset event of IEEE1394. The Unit (or Subunit) identifier descriptor discovery application will query capabilities of target devices (e.g. ability of Digital TV to display on-screen setup commands) using the AV/C Read Descriptor Command.

5.5.3 Description of Specific Protocols

This section describes the specific protocols used in the protocol stacks identified above.

5.5.3.1 IEEE 1394 Physical Layer

Defined in IEEE 1394-1995, IEEE 1394a-2000, and IEEE 1394b-2002.

5.5.3.2 IEEE 1394b

Physical Layer for the IEEE 1394b backbone is defined in Section 5.1.

5.5.3.3 IEEE 1394 Link Layer

Defined in IEEE1394-1995, IEEE 1394a-2000, and IEEE 1394b-2002.

5.5.3.4 IEEE 1394 Transaction Layer

Defined in IEEE1394-1995, IEEE 1394a-2000, and IEEE 1394b-2002.

The devices conforming to this specification shall be asynchronous transaction capable.

5.5.3.5 IEEE 1394 Serial Bus Management

Defined in IEEE1394-1995, IEEE 1394a-2000, and IEEE 1394b-2002.

Regarding Command and Status Registers (CSRs), the implementation of both CSR Architecture core registers and Serial-Bus-Dependent registers shall conform to IEC 61883-1.

Regarding Configuration ROM, the implementation of Bus_info_Block, root_directory and unit_directories shall conform to IEC 61883-1.

The support of Isochronous Resource Manager capability is recommended. The support of Bus Manager capability is optional.

5.5.3.6 Function Control Protocol (FCP)

Defined in IEC 61883-1.

The devices conforming to this specification shall implement a Command Register and a Response Register as the target address space of command frame and response frame, respectively. The register address, frame structure and CTS (Command/Transaction Set) value shall conform to IEC 61883-1.

5.5.3.7 AV/C READ DESCRIPTOR Command

Defined in AV/C Digital Interface Command Set General Specification Version 4.2.

AV/C devices conforming to this specification should support the AV/C READ DESCRIPTOR command to issue or respond to queries using the Subunit identifier descriptor.

5.5.4 Internet Protocol (IP)

The protocol stack for Internet Protocol (IP) is defined in Figure 5

This protocol stack realizes terminal or router functions using related IP protocols.

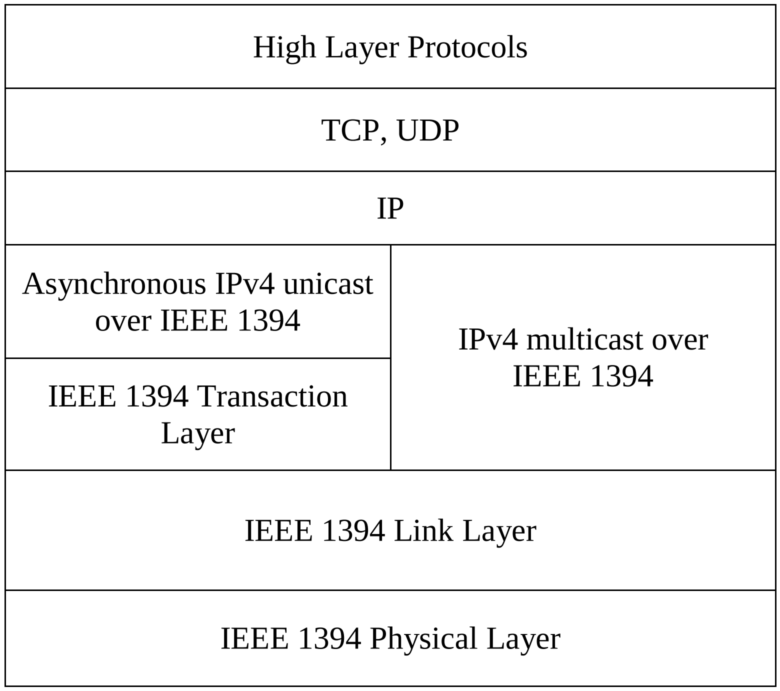


Figure 5 – Protocol Stack for Internet Protocol

6 Addressing, Discovery, and Control

6.1 Heterogeneous Networks

The VHN Home Network is an Internet of several heterogeneous networks (see Figure 2). A common internetworking protocol is thus needed to enable communication among all devices on the home Internet. This section of the specification describes the protocols necessary for all devices to be configured and to communicate using the network protocol.

6.2 User-to-Device Control

User-to-device control is specified in VHN by reference to ANSI/CEA-2027-A, “A User Interface for Home Networks Using Web-based Protocols.” An overview of ANSI/CEA-2027-A is presented in Annex D for information.

6.3 UPnP

UPnP Version 1.0 shall be incorporated by reference into this standard. An overview of the UPnP architecture is presented in Annex E. UPnP includes provision for device-to-device control under the Control and Eventing specifications.

UPnP Version 1.0 shall be implemented in VHN for:

- Addressing

- Discovery
- Description
- Control and Eventing
- Presentation (if needed)

A VHN device shall operate according to the UPnP Device Architecture 1.0 requirements for device discovery and control. A VHN device shall assign IP addresses based on the Dynamic Configuration of IPv4 Link-Local Addresses (IETF Internet draft) and shall include a DHCP client and a DNS client (all cited in Section 2.2). A VHN device supporting IPv6 shall comply with Annex A–IPv6 Support specified in the UPnP Device Architecture.

7 Media Transport

7.1 Streams

Streams shall be implemented in VHN by reference to Annex A of ANSI/CEA-2027-A, "A User Interface for Home Networks Using Web-based Protocols," and to UPnP AV Architecture (UPnP AV). The latter specifically applies to streaming IP networks, typically based on the Ethernet protocol. ANSI/CEA-2027-A applies to IEEE 1394-based networks for management of the isochronous streams.

7.1.1 Isochronous Streams in ANSI/CEA-2027-A

Annex A of ANSI/CEA-2027-A references AV/C commands. IEEE 61883, Part 4 specifies the application of MPEG Level 2 System transport on an IEEE 1394 bus.

7.1.2 IP-based Streams in UPnP AV

The combination of the UPnP Device Architecture and the AV Device Control Protocols provides the necessary methods for stream control. Within the UPnP Forum, the AV work group created the UPnP AV specification that describes the binding of streams by UPnP AV devices. This document is incorporated by reference.

The UPnP Device Architecture defines an infrastructure upon which device classes can be built. One such device class is Audio/Video (AV). The UPnP AV specification defines a procedure for controlling various UPnP AV devices. A high level overview can be found in the UPnP AV Architecture specification.

The UPnP concept for AV playback incorporates a control point and two types of AV devices:

- A Media Server that acts as the source for the media content to be played.
- A Media Renderer that is used to render the content.

A Control Point coordinates all the interactions between Media Servers and Media Renderers. Although the Control Point coordinates the interaction between these devices, it does not specify the communication protocol used between them. A block diagram of the device interaction is shown in Figure 6. The Media Servers, Media Renderers and Control Points can exist physically as three separate entities, all can coexist in one physical device, or in any other intermediate combination.

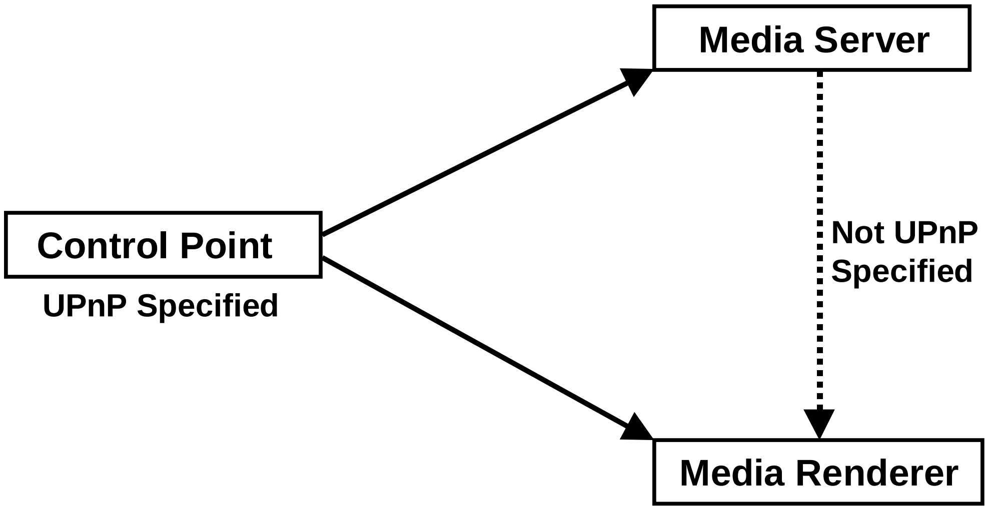


Figure 6 – UPnP AV Streaming

The Media Server has a Content Directory Service, a Connection Manager Service, and may have an AVTransport Service. The content on the Media Server can be browsed or searched using the Content Directory Service. The Media Renderer has a Rendering Control Service, a Connection Manager Service, and also may have an AVTransport Service. Details may be found in in the UPnP AV Architecture specification.

The following is a typical playback scenario abstracted from the UPnP AV Architecture specification:

1. The Control Point uses the UPnP discovery protocol to find the Media Server and Media Renderer.

2. The Control Point then uses the Browse or Search actions of the Content Directory Service to find the content of interest.

3. Included in the metadata returned from the browse or search is the available media formats and protocols.

4. The Control Point queries the Media Renderer using the GetProtocol action in the Connection Manager Service.

5. The formats and protocols returned from the GetProtocol action are then compared, and a transfer protocol supported by both the Media Server and Media Renderer is selected.

6. Once the Control Point establishes a connection between the Media Server and Media Renderer, it cannot interact in the process any further unless the PrepareForConnection action of the Connection Manager Service and the AVTransport Service are implemented. In this case it is also possible for multiple streams to be controlled.

The UPnP Device Architecture and AV Device Class comprise a completely open system. The UPnP Device Architecture and AV Device Class simply provide a framework and protocol that allows devices and control points to find each other and to setup communications links between them. This procedure enables streaming media between devices. The system does not define nor is dependent on any particular transfer mechanism or network type.

7.1.3 Routing IP streams

A router inserted in a VHN network configured for IP-based streaming shall support the minimum requirements of the UPnP Internet Gateway Device.

7.1.4 Media Devices for IP Streaming

A VHN Media Device on an IP-based streaming network shall conform to UPnP AV Architecture.

A VHN Media Server on an IP-based streaming network shall support the minimum requirements of the UPnP Media Server and shall include Content Directory Service support for the Search action.

A VHN Media Server on an IP-based streaming network shall support the requirements of three-character language identifiers according to IETF RFC 3066 in the UPnP Content Directory. Two character language identifiers shall be used in the Content Directory, unless such language identifiers are only available in a three-character format.

A VHN Media Player on an IP-based streaming network shall support the minimum requirements of the UPnP Media Renderer. A VHN Media Player on an IP-based streaming network shall additionally support the minimum requirements of the AVTransport Service and shall act as a UPnP control point for the ContentDirectory AV Service.

The Control Point function shall be able to browse as well as search a Content Directory. A VHN Media Player on an IP-based streaming network capable of audio amplification should include the following Media Renderer actions: GetMute, SetMute, GetVolume, SetVolume. A VHN Media Player capable of on-board video display (such as a television set) should include the following Media Renderer actions: GetBrightness, SetBrightness, GetContrast, SetContrast, GetSharpness, SetSharpness

A VHN Media Player should be capable of interpreting the language property of an item in the UPnP Content Directory as a two or three-character identifier as specified in IETF RFC 3066.

A VHN Media Controller on an IP-based streaming network shall be a UPnP Control Point for the following UPnP AV Services:

- AVTransport
- ContentDirectory
- ConnectionManager
- RenderingControl

A VHN Media Controller on an IP-based streaming network may be a UPnP Control Point for the UPnP IGD Services.

7.1.5 Media Transport for IP Streaming

This section describes network protocol requirements for content streaming and file transfer to a VHN device on an IP-based streaming network.

7.1.5.1 Media Streaming

A VHN Media Device on an IP-based streaming network shall support HTTP/1.1 over TCP for media streaming and file transfer. A VHN Media Server shall support byte-range HTTP requests as documented in HTTP/1.1.

A VHN Media Device on an IP-based streaming network should support RTSP on TCP using RTP and RTCP over UDP streaming method.

NOTE: A VHN Media Device may support the additional media streaming methods, such as:

- HTTP 1.1 over UDP
- RTSP over TCP with interleaved RTP payload
- RTSP/RTP tunneled within HTTP 1.1 over TCP
- SDP to describe an RTSP session as documented in RFC 2326 Appendix C
- SDP to describe the content parameters of a HTTP GET

A VHN Media Device supporting additional media streaming protocol shall not interfere with the required methods.

When using HTTP over TCP for streaming, the HTTP GET method shall be used by the VHN Media Player to request a content stream from the VHN Media Server. The VHN Media Player may terminate this stream by dropping the connection to the VHN Media Server at any time.

NOTE: Only start and stop transport control over the network is possible with this method. However, a VHN Media Player may use stream-buffering methods to offer transport control within the segment of the stream that exists in the buffer.

If a VHN Media Server allows streaming of live content, it shall represent the live stream as a Universal Resource Identifier (URI) in its UPnP ContentDirectory.

NOTE: VHN Media Server mechanisms for real-time capture and buffering of live media streams for transmissions via HTTP are implementation-specific and outside the scope of this specification.

7.1.5.2 Media File Transfer

During a file transfer operation, a VHN Media Player or Media Controller on an IP-based streaming network shall set up the transfer with UPnP ContentDirectory Service methods. When using HTTP over TCP for media file transfers, the HTTP GET method shall be used by the VHN Media Device requesting a file. A VHN Media Server shall support the byte-range HTTP requests documented in HTTP/1.1.

7.1.6 Quality of Service

A VHN Network Switch on an IP-based streaming network shall support IEEE 802.1q and CEA-2007. A VHN Host Device should support these same standards. Specific requirements for handling the priority data are described in this section.

NOTE: VHN does not provide quality of service guarantees on an IP-based streaming network; rather, it provides common methods for improving quality of service over an IP-base streaming network.

7.1.6.1 VHN Media Player

VHN Media Player supporting 802.1q Priority Levels shall conform to the following Priority Level requirements:

- It shall include Priority level 011 in all UPnP communication for AVTransport, Rendering Control, and Connection Manager Services via HTTP.
- It shall, by default, include user Priority Level 010 in all media requests via HTTP GET and RTSP PLAY commands.
- Players supporting RTP/RTSP shall include user Priority Level 011 for all RTSP, RTCP, and SDP communication, except for RTSP PLAY commands.
- A VHN Media Player should allow users to change the default Priority Level for all media requests via HTTP GET and RTSP PLAY commands. Such a configuration option shall only allow Priority Levels 000, 001, and 010. If a Priority Level changes during stream playback, it should not cause playback to reset at the beginning.

7.1.6.2 VHN Media Server

VHN Media Servers supporting 802.1q Priority Levels shall conform to the following Priority Level requirements:

- It shall include user Priority Level 011 in all UPnP communication for AVTransport, Rendering Control, and Connection Manager Services via HTTP.

- It shall, by default, include user Priority Level 010 in all responses to incoming media requests via HTTP GET and RTSP PLAY commands.

- Servers supporting RTP/RTSP, shall include user Priority Level 011 for all RTSP, RTCP, and SDP communication, except for RTSP PLAY command.

- It shall check the Priority Level of all incoming media requests via HTTP GET and RTSP PLAY commands, and use the same Priority Level in the server's response containing the media payload. If the request contains no Priority Level, then the server's HTTP response should use the server's default Priority Level.

- A VHN Media Server should allow users to change the default Priority Level for all incoming media requests via HTTP GET and RTSP PLAY commands that contain no Priority Level. Such a configuration option shall only allow Priority Levels 000, 001, and 010.

7.1.6.2.1Serving Full Quality Streams

Prior to serving a request for content, a VHN Media Server should ensure that it can provide the necessary resources to serve the outbound stream at a speed equal to or faster than that required for full-quality playback of the content in real time.

Upon any new network media request, the server should refuse transmission of content if the required transmission speed cannot be provided. This performance requirement for a VHN Media Server is limited to the internal system, and not subject to network limitations.

NOTE: For example, a VHN Media Server would allocate enough internal system bandwidth to ensure transmission of an MPEG-2 main profile @ main level transport stream, perhaps at 15Mbps or the maximum bit rate of the entire stream, if known.

7.1.6.3 VHN Network Switch

A VHN Network Switch on an IP-based streaming network shall preserve pre-existing Priority Levels in any inbound frames. Such pre-existing Priority Levels shall not be modified prior to retransmission. A VHN Network Switch shall retransmit all frames in the order of priority.

7.1.6.4 VHN Network Router

A VHN Network Router on an IP-based streaming network shall preserve Priority Levels with an origin and destination within the same subnet. A VHN Network Router may be configured to allow Priority Levels for packets originating from an internal subnet and destined for an external address to be included when the packets are forwarded to the WAN port. If a VHN Network Router can allow the forwarding of Priority Levels across subnets, the router's default configuration shall be to disable Priority Level forwarding.

7.2 Telephony

Telephony services, if present, in VHN are specified by reference to CEA-851.1, "IP-Based Digital Telephony for the Versatile Home Network." An overview of CEA-851.1 is presented in Annex F for information.

8 Backbone Interfaces

8.1 Backbone-Component Interface

Backbone-Component Interfaces provide a physical connection between the VHN Home Network and a component network, such as an in-room Ethernet, an IEEE 1394 cluster of A/V devices, or a home automation system using powerline to distribute commands to appliances in the home. The Backbone-Component Interfaces may implement address translation or protocol conversion.

A Backbone-Component Interface will usually require two protocol stacks: One for the backbone (always the VHN Home Network stack), and the other for the component network. An example is shown below of protocol stacks in a Backbone-Component Interface that connects the VHN Home Network backbone (implemented on plastic optical fiber) to a 10BASE-T Ethernet, where both support UPnP.

Protocol Layer	VHN Backbone	Ethernet Component Network
Layers 5-7 (Application)	VHN Home Network Messaging in UPnP	VHN Home Network Messaging in UPnP
Layer 4 (Transport)	TCP	TCP
Layer 3 (Network)	IP	IP
Layer 2 (Data Link)	IEEE 1394b (long-distance)	IEEE 802.3 (10BASE-T)
Layer 1 (Physical)	POF Interface	UTP Cat 5 Interface

Figure 7 – Example of Protocol Stacks in a Backbone-Component Interface

In general, it is preferable that a Backbone-Component Interface be implemented at the lowest layer common to both technologies. In general, this means that the Backbone-Component Interface will operate at Layer 3 or higher in the protocol stack. An interface that operates at Layer 3 is called a *router*; an interface that operates at a higher layer is often called a *gateway*.

The special instance in which the interface device may operate at Layer 2 is treated in Section 8.1.1 below.

The decision to use a router or a gateway to implement the Backbone-Component Interface is usually dictated by the Layer 3 technology of the component network. If the component network implements IP, the Backbone-Component Interface can be a router. This may apply, for instance, if the component network is a version of Ethernet or Token Ring. If the component network *does not* implement IP, the Backbone-Component Interface shall be a gateway.

With the exception noted below in Section 8.1.1, this standard does not further specify the technology to be used in implementing Backbone-Component Interfaces.

8.1.1 IEEE 1394 Bridging

Because the backbone of the VHN Home Network uses IEEE 1394b-2002, the long-distance version of IEEE 1394, special considerations apply when the component network also implements a version of IEEE 1394. In this unique instance, the Data Link layers are the same for both the backbone and component networks. That means that the Backbone-Component Interface can be implemented using IEEE 1394 bridging, which may be both faster and less expensive than using routers or gateways. If the component network is also uses IEEE 1394b, the Backbone-Component Interface may be implemented at the physical layer, using a repeater.

IEEE 1394 bridging is defined in IEEE 1394.1-2004, which is included in this standard by reference. All IEEE 1394—IEEE 1394 bridges shall conform to the requirements in IEEE 1394.1-2004.

Requirements for implementing IEEE 1394—IEEE 1394 Backbone-Component Interfaces, are given below.

8.1.2 Requirements for IEEE 1394—IEEE 1394 Interfaces

When the component network uses IEEE 1394—IEEE 1394 or IEEE 1394a-2000 technology, the interface between the backbone and the IEEE 1394 component network shall be the bilingual port electrical and signalling interface specified in IEEE 1394b. The bilingual port supports speeds up to S100 when the backbone medium is Category 5 UTP, S200 when the backbone medium is 50m Plastic Optical Fiber, and S3200 when the backbone medium is Glass Optical Fiber.

This implementation requires an IEEE 1394—IEEE 1394 bridge, which is capable of performing the protocol conversion between IEEE 1394a and IEEE 1394b at the interface between the backbone and the component network. The implementation of such a function may be powered from the IEEE 1394 component network, in which case it shall consume no more than 3W of power (power class 4). The implementation of such a function shall comply with all appropriate buildings wiring and safety requirements.

When the component network uses IEEE 1394b, the Backbone-Component Interface may be implemented using an IEEE 1394 repeater. However, improved performance may be obtained by using IEEE 1394-1394 bridges, particularly for bandwidth isolation. Typically, such bridges may be implemented at the interface between the component network when this is IEEE 1394 and the backbone, and/or at the center of the star, as described in Section 8.1.1 above.

Communication across an IEEE 1394—IEEE 1394 bridge is normally possible only if the two communicating IEEE 1394 devices are "bridge aware" (in some applications, only one of the two devices need be bridge aware). It is strongly recommended, but not required in this standard, that all IEEE 1394 devices implement the features specified in IEEE 1394.1-2004 necessary to be bridge aware.

8.2 Access Interfaces

8.2.1 Installing an Access Interface

Access Interfaces are devices that mediate between the access network and digital home network protocols. An example of an access interface is a POTS modem, an ISDN adapter, a cable modem, a DBS decoder, or a Residential Gateway. The access interface uncouples the technologies of the access networks from the in-home networks, mediates between the different network protocols, and establishes a platform to enable creation and introduction of new services and capabilities.

As the access interface is not an intrinsic element of the VHN Home Network, some features and capabilities of the access interface, such as those associated with termination and mediation of access services, may overlap with those of the VHN. This overlap will most likely impact the overall functionality of the involved service or capability if the access interface and VHN are deployed simultaneously.

It is recognized that some access interfaces (e.g., a cable modem) may be implemented before a VHN is installed in the home; similarly, a VHN may be implemented independently, and subsequently an access interface (e.g., a Residential Gateway) may be installed. In either case, the VHN and the access interface must be capable of functioning both independently and harmoniously when used together. Note that interoperability may involve *future* requirements that the VHN incorporate a means to eliminate, bypass, or disable features that are redundant with those of the access interface.

VHN should accommodate Access Interfaces based on ISO/IEC 15045, "Residential Gateway." Key features of this standard are included in Annex G for information. Also, VHN should allow a UPnP gateway. However, note that UPnP does not specify a firewall, as recommended in the next section.

8.2.2 Network Security: Firewalls, Conditional Access, Privacy Management

A VHN Home Network will provide full connectivity between networked devices in the home; when combined with access interfaces, this connectivity results in enhanced telecommunications capabilities. VHN devices can be controlled from remote locations, and can be the source or destination of broadband audio and video streams.

With the home "opened up" in this manner, protection practices are quite important. Such practices are necessary to protect the privacy of network data in MIBs (database for management information) and the privacy of user data in other storage facilities, and to protect the home network from outside tampering. There is also a need for service providers to guard against unauthorized access to their services, and for access providers to protect their access networks from tampering or from harm.

There are thus four entities that require protection:

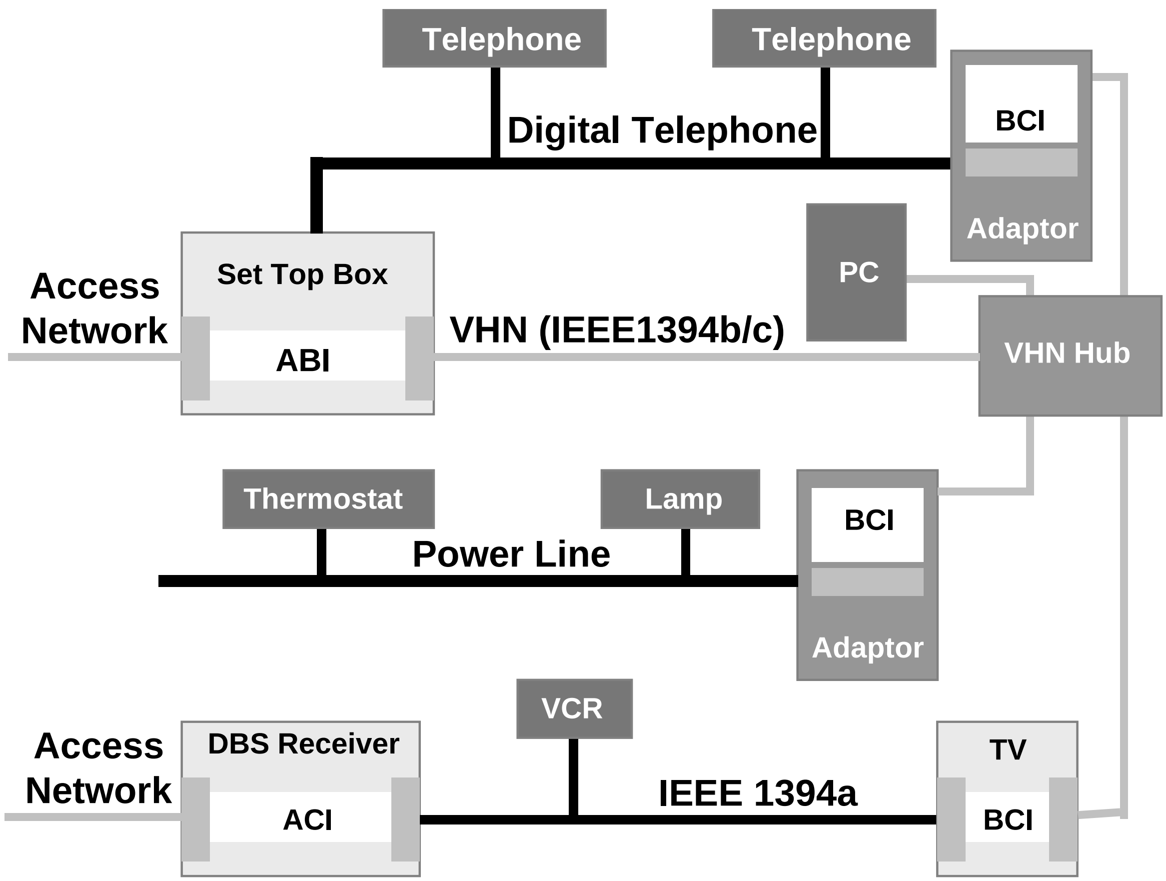
- The digital home network, which must be free from tampering
- The user data stored on networked devices, which must be protected from prying
- The service provider, who must ensure that only authorized services are accessed
- The access network, which must be secured from tampering or from physical harm

CEA-852.2, “Security Services for the Versatile Home Network,” addresses these issues of privacy and security for home networks, and is incorporated by reference. CEA-852.2 specifies provisions for a firewall that shall be incorporated in any access interface between and home network and the Internet. These requirements are accommodated if the Access Interface conforms to the ISO/IEC 15045 residential gateway, as recommended in Section 8.2.1.

Annex A Examples of VHN Home Network Implementations

A.1 Example 1 – A VHN Home Network with CATV, DBS, and POTS Access

The first example (Figure 8) shows multiple access networks coming into the home, both through the VHN backbone and through an IEEE 1394a-2000 Component Network. The set top box that connects the access network (cable TV) contains an access-to-backbone interface. The TV contains both an IEEE 1394a-2000 and an IEEE 1394b-2002 connection, and thus contains a backbone-to-component interface. In this example, digital telephone service is delivered over the cable and terminated on the Set Top Box (STB). Adapters are plugged into the VHN to provide conversion from Component Networks (telephone and power line) to the VHN backbone. The protocol conversion may include media, and all seven layers of the protocol stack.



ABI = Access-Backbone Interface
ACI = Access-Component Interface
BCI = Backbone-Component Interface

Figure 8 – A VHN Home Network with CATV, DBS, and POTS Access

A.2 Example 2 – A VHN Home Network with a Residential Gateway

This example (Figure 9) is similar to the previous one, except that a Residential Gateway (RG) is used. The Residential Gateway is a flexible access device that will allow multiple access networks to connect to the home network. Each access network will terminate in the Residential Gateway on a customized access network "card." In this example an ADSL card and a CATV card are installed. On the "home" side of the RG are a VHN Home Network card, a POTS card (analog), and a CEBus card (for power line carrier communications). Because the Residential Gateway implements three types of VHN connections (backbone, access and component network), it must contain three VHN interfaces: access-to-component, backbone-to-component and access-to-backbone.

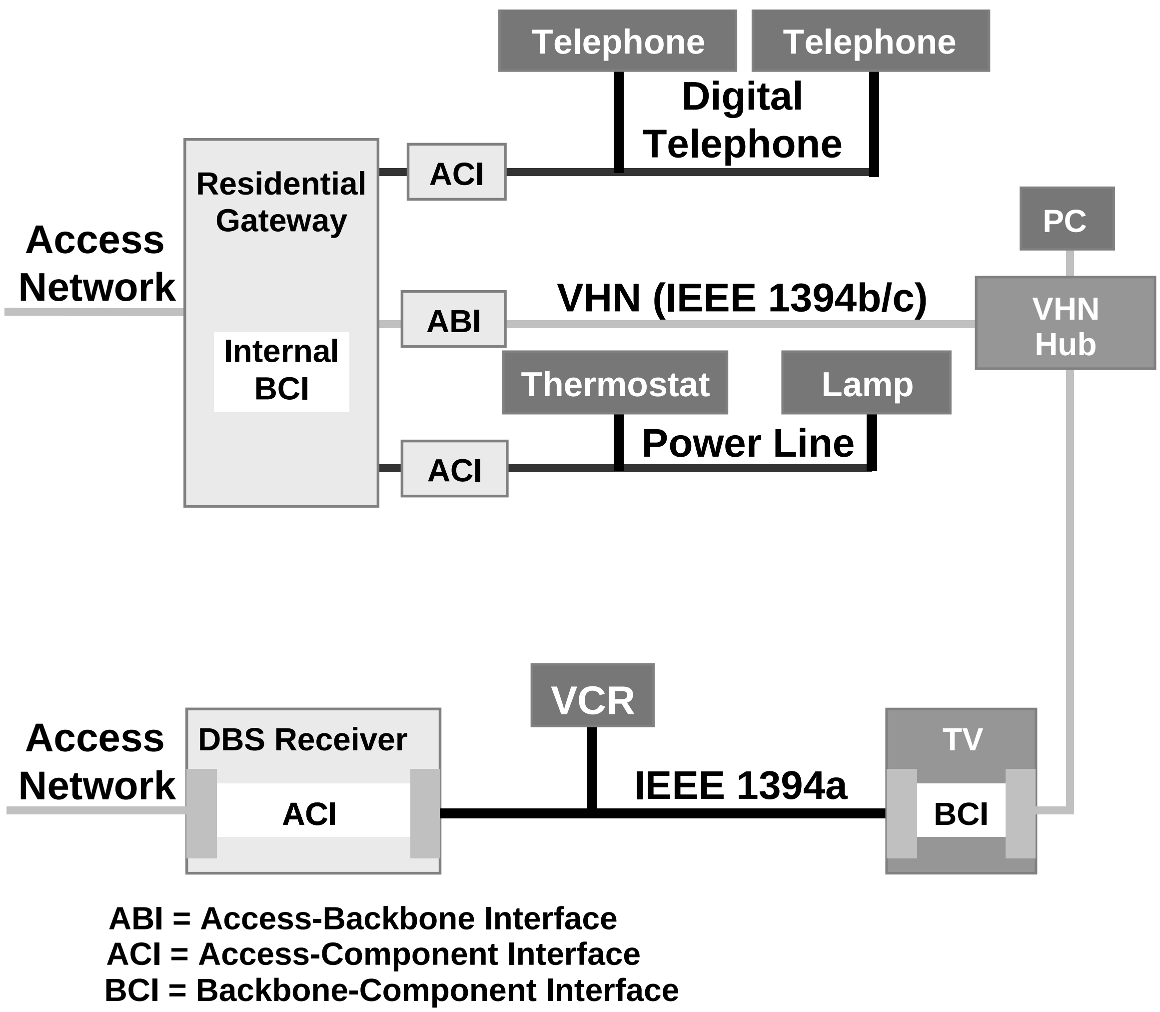


Figure 9 – A VHN Home Network with a Residential Gateway

A.3 Example 3 – A VHN Home Network with a Multimedia Hub

In this example (Figure 10) the hub of the VHN Home Network backbone is integral with an access device (in this case, a set-top box/gateway). We call this arrangement a "multimedia hub." This hub could also have an integral cable modem and tuners. Only one VHN interface is required since the hub plugs only into the backbone. The adaptation to the Component Networks is done in this example through a cable with a "lump" containing electronics, or with electronics at either end. Note how this implementation simplifies the overall complexity of the home network, as the hub is integrated with the cable modem and tuner. The additional expense of Component Network adaptation in this case is borne only by the unique adapters, thus keeping the initial cost low.

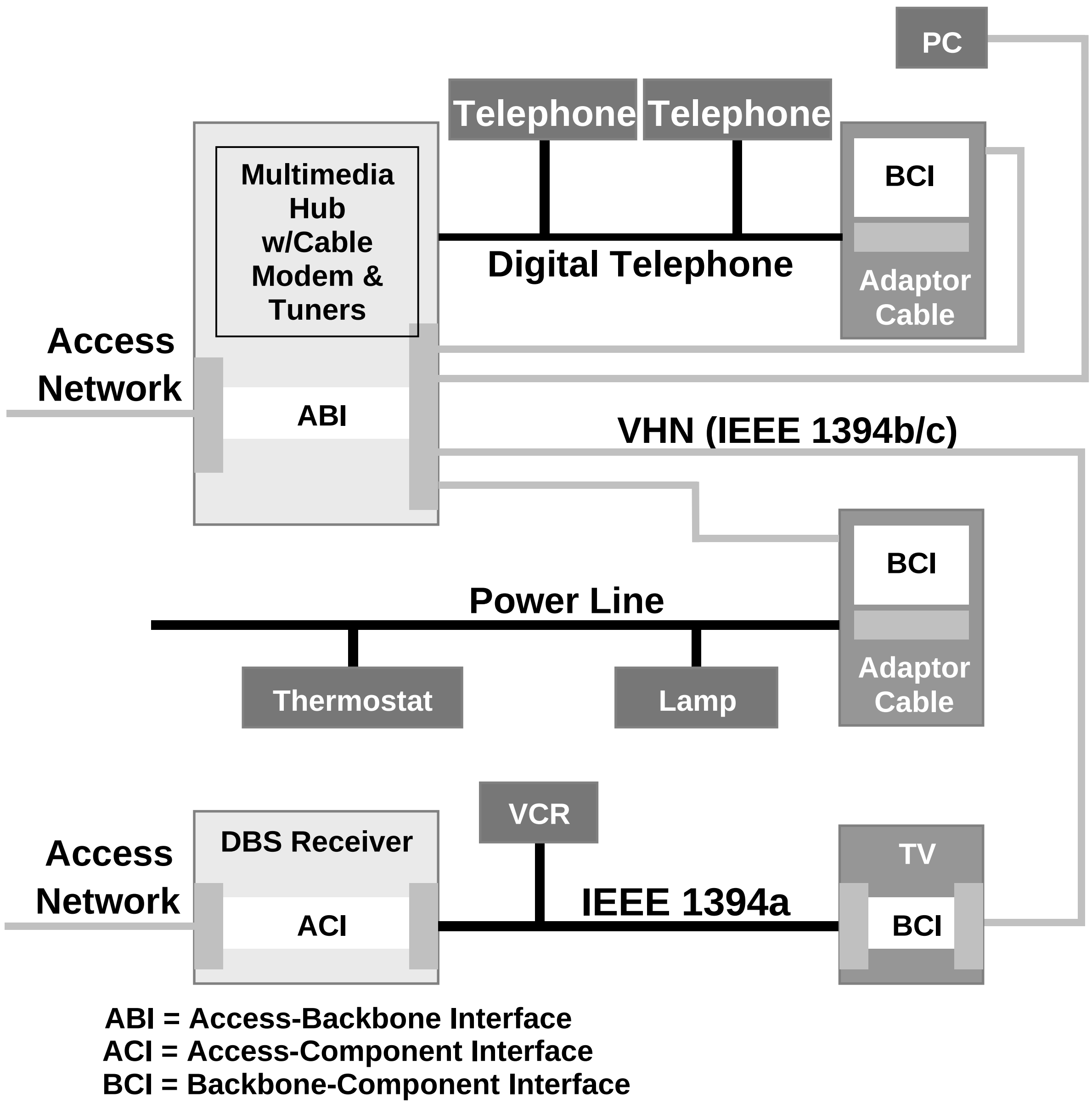


Figure 10 – A VHN Home Network with a Multimedia Hub

Annex B - Introduction to IEEE P 1394c (Informative)

The following overview of IEEE P1394c was obtained from www.ieee.org in November 2004. Balloting for this proposed standard is planned for the winter of 2004-2005.

“This is a full-use standard whose scope is to provide an amendment to IEEE Std 1394-1995™, IEEE Std 1394a-2000™ and IEEE Std 1394b-2002™ that defines features and mechanisms that provide gigabit speed using category 5 cabling over single hop distances of up to 100M. The following are included in this amendment:

1. Automatic negotiation that allows a port to connect using either the IEEE Std 1394 or IEEE Std 802.3 higher layers;

2. An updated beta port specification that provides easy connection with the same PHY specified in IEEE Std 802.3 clause 40; and

3. Various minor updates to IEEE Std 1394b-2002™.”

Annex C - The OSI Reference Model (Informative)

In the early 1980's, the *International Organization for Standardization* (ISO) completed a project to define an Open Systems Interconnection (OSI) Reference Model for the connection of computers through LANs (Local Area Networks) and WANs (Wide Area Networks). While few real telecommunication systems actually conform to the OSI Reference Model specification in detail, the seven-layer OSI model has become a standard for describing data communications systems. Discussions of transmission technologies usually include descriptions of how the system in question conforms to, or differs from, the OSI reference model.

OSI defines any computer communication system in terms of seven layers (see Figure 11). All seven layers reside in each end-user device in a communication system; intermediate devices, such as bridges and routers, contain a subset of the seven layers. From the top down, the OSI layers are:

- Application Layer (Layer 7)

  This is the layer that is "visible" to the user, or to the user's application program. The structure of the OSI Reference Model hides the operation of the lower layers from the Application Layer, so that users and application programs do not have to be concerned with the details of the communications system.

- Presentation Layer (Layer 6)

  The Presentation Layer is concerned with maintaining the meaning of data that may be represented differently on the communicating computers. For example the source computer may be running a program that stores numbers in two's-complement form, while the receiving computer uses one's-complement; it is the responsibility of the Presentation Layer in each end system to ensure that the number is represented correctly.

- Session Layer (Layer 5)

  The Session Layer organizes the "dialog" between the communicating end systems. For example, it determines whether both systems may talk simultaneously, or whether they will alternate talking and listening, and if so, what the interrupt points will be.

The higher three layers are concerned with the manipulation and storage of data in the end system; they are often combined into a single "application layer," to distinguish their functions from those of the lower four layers, which are more directly concerned with communications:

- Transport Layer (Layer 4)

  The Transport Layer is the lowest of the seven layers that appears only in end-user systems. It interfaces the higher layers with the actual communication facility that is embodied in the lower layers. The Transport Layer is responsible for setting up reliable communications between end-users and ensuring correctly-sequenced error-free transmission of user information.

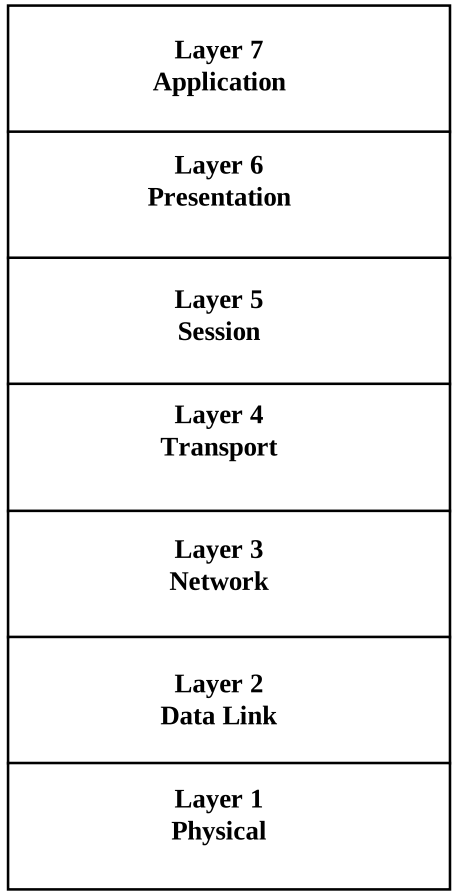


Figure 11 – OSI Reference Model

- Network Layer (Layer 3)

  The Network Layer routes user information, in the form of packets, from the source system to the destination system, sometimes using the facilities of many intermediate systems. The connection between any two systems is called a link; the network layer routes packets over as many links as necessary to reach the destination system. The network layer is responsible for determining a route through the network, and for shielding the higher layers from the details of route planning and message delivery.

- Data Link Layer (Layer 2)

  The Data Link Layer moves information between two systems over a single link, in the form of a datagram or frame. In IEEE 802.x LANs (such as Ethernet or Token Ring), the Data Link Layer is divided into two sublayers, the Logical Link Control (LLC) sublayer and the Medium Access Control (MAC) sublayer. The LLC sublayer, which is common to all IEEE 802.x LAN technologies (and some others), determines the physical address of the next destination (which may be an intermediate system), and assembles the data packet into a frame with the correct address and with error control and start and stop sequences to delimit the frame. The MAC sublayer in most cases distinguishes one LAN technology from another; it negotiates the insertion of the frame onto the physical medium. The medium access strategies used by various LAN technologies are the most important distinguishing characteristics of those technologies.

- Physical Layer (Layer 1)

  The Physical Layer is concerned with transporting bits between one device and another. The physical layer in the transmitting system inserts onto the physical medium an appropriate physical analog of the logical bit pattern of the frame. This analog may be in the form of a voltage or a burst of electromagnetic radiation. The receiving Physical Layer detects this pattern, corrects for noise and distortion, and interprets the resulting signal as a one or zero.

Each layer in the source device sends a message, called a Protocol Data Unit (PDU), to the corresponding layer in the destination device using the services of the next-lower layer to send the message. Thus, for example, a program operating in the Network Layer (layer 3) of the source system (called a *network entity)* sends a Network PDU (often called a *packet*) to a *peer network entity* running in the Network Layer of the destination system. It does this by passing a Network PDU to the next lower layer, the Data Link Layer (Layer 2). The Data Link Layer accepts the Network PDU as a Data Link Layer *Service Data Unit* (SDU), to which it adds *Protocol Control Information* (PCI), forming a Data Link Layer Protocol Data Unit (PDU), often called a *frame*. The original Network PDU was formed by adding Network PCI to a Network SDU, which originated as a Layer 4 (Transport Layer) Protocol Data Unit.

The process is reversed in the destination system: The Data Link Layer PDU is received by the destination Data Link Layer, having been passed up by the destination Physical Layer. The Data Link Layer removes the Data Link Layer Protocol Control Information (PCI), producing a Data Link Layer SDU. This Data Link Layer SDU is passed up to the destination Network Layer, where it is received as a Network PDU; the Network Layer removes the Network Layer PCI, producing a Network SDU, which it passes up to the destination Transport Layer as a Transport Layer PDU.

Annex D - ANSI/CEA-2027-A User Interface (Informative)

D.1 Overview of ANSI/CEA-2027-A

In July 2004 the Consumer Electronics Association (CEA) completed an important standard for user control of audio/video (A/V) equipment interconnected via a home network. The official designation of this standard is ANSI/CEA-2027-A, "A User Interface for Home Networks Using Web-based Protocols," available from Global Engineering Documents, http://global.ihs.com.

ANSI/CEA-2027-A specifies an A/V network where user control is exercised via a remote control unit (RCU) plus an on-screen display of graphics, icons, and text. The display presents information about the components and options for directing source material to desired output devices. The user makes selections via the RCU. This standard was updated from ANSI/CEA-2027 to ANSI/CEA-2027-A to incorporate proxy services for AV/C devices and Ethernet.

The user interface combining a display menu and an RCU is familiar to consumers. Most VCRs use on-screen programming for setting up a recording session. The screen display consists primarily of text on a blue screen. ANSI/CEA-2027-A enhances the typical VCR display format by adopting concepts from the World Wide Web and applying them to all the A/V components, not just the VCR. Each component has the option of presenting relevant information to the user on a TV as a web page.

ANSI/CEA-2027-A defines the rules for delivering component data to a TV and to an RCU without specifying details about the "look and feel." The CEA standards committee left considerable flexibility for manufacturers to create unique user interfaces, while promoting interoperability among components across brands.

This material is excerpted from the following article, where additional information about this standard, including illustrations, is available:

> "Consumer-Friendly Audio/Video Networking," by Kenneth Wacks, Ph.D., *iHomes & Buildings*, Winter 2004, Volume 1, Number 3, pp 13-15, free download at www.caba.org.

D.2 An A/V Home Network

ANSI/CEA-2027-A defines a unified control scheme for networked A/V devices. Some devices include a combination of functions, such as a TV and a video recorder. In those cases, one physical device is treated as multiple Logical Units for network control. Each manufacturer decides which device features are accessible via remote control. Each device contains data in the form of a web page that describes the device features. No central network database is required.

The ANSI/CEA-2027-A user interface consists of one or more TV displays plus an RCU that presents a consistent set of data for managing Logical Units remotely via a home network. This standard refers to the displays as Renderers. It is expected that the Renderers will be Digital TVs (DTVs), although other displays including PCs (Personal Computers) and PDAs (Personal Digital Assistants) are possible.

Annex A of ANSI/CEA-2027-A uses the IEEE-1394 bus for interconnecting A/V components. IEEE-1394 is a wired network that carries control messages plus streams of audio and video signals. Extensions of CEA-2027-A are planned for Ethernet.

D.3 A/V Control

The Basic Operations enabled by ANSI/CEA-2027-A include:

- Determining which devices are accessible via the home network.
- Selecting a device to control.
- Enabling the user to learn what functions in the selected device can be observed or controlled.
- Viewing or controlling elements in the selected device.

Annex E - UPnP Architecture (In formative)

E.1 Overview of UPnP

The UPnP™ Device Architecture is a network architecture created by Microsoft Corporation as Universal Plug and Play to enable communications among appliances, devices, and personal computers. Nodes on a UPnP network are classified as Controlled Devices or Control Points. The UPnP specification is now managed by the UPnP Forum

Controlled Devices act as servers that respond to requests from Control Points. The major features of UPnP can be divided into the following categories:

- Network configuration
- Association control
- Messaging and event notification

The methods chosen for each category of service are described. A common thread is the dependence on Internet protocols including TCP/UDP/IP, HTTP, and XML.

UPnP does not define a complete communications protocol. There are no specifications for the Physical Layer (the communications medium) or the Data Link Layer, using the terms for Layers 1 and 2 defined by the OSI Reference Model for Communications. The UPnP specification stresses that it requires no dependence on any programming language or operating system. However, communication protocol specifications do not usually address these issues, which are product-dependent. Devices programmed with various languages and running on various operating systems internally may, nevertheless, exchange messages and data as long as they conform to the same external communications protocol.

The UPnP Forum is a private consortium of 720 companies (as of October 2004) that have signed a contract to pool intellectual property. Membership in the UPnP Forum is free. The UPnP Forum provides public information at www.upnp.org. Some UPnP Forum members have formed the UPnP Implementers Corporation (www.upnp-ic.org) to develop interconnectivity specifications, including testing and certification procedures. Also, the UPnP IC administers the UPnP logo program. The UPnP IC owns the UPnP trademark.

E.2 Network Configuration

E.2.1 Address Acquisition

A node acquires a network address at this stage. Two methods are defined: managed and unmanaged.

E.2.1.1 Managed Device Addressing

In a managed environment, a server (known as a Dynamic Host Configuration Protocol server, or DHCP server) assigns an IP (Internet Protocol) address to the device. Each device must contain a DHCP client in order to communicate with the DHCP server for address acquisition.

E.2.1.2 Unmanaged Device Addressing

The Auto IP procedure selects an IP address automatically from a pool of reserved addresses. The device tests the availability of an IP address by issuing an Address Resolution Protocol (ARP) probe to determine if any other device responds to that address. A device configured using Auto IP must check every few minutes to determine if a DHCP server has become available. When a DHCP server is found, the device assumes the DHCP-assigned address and may relinquish the Auto IP address.

E.2.2 DNS Option

Once a numeric IP address has been acquired, it may be translated to a familiar name using the services of a Domain Name System (DNS). This is the mechanism for assigning English-like URLs (Universal Resource Locators) in place of numeric IP addresses for accessing web pages.

E.3 Association Control

E.3.1 The Participants in Association Control

The purpose of association control is to relate the functions of one device to another so the devices can cooperate to provide services. Association control in UPnP includes Discovery, Description, and Presentation. Association in UPnP is defined to occur between devices and Control Points. Control Points are defined explicitly in the UPnP specification. If an application such as lighting is configured with a group of sensors, switches, and fixtures, the lighting controller could serve as the Control Point. However, in a fully distributed network, any device such as an appliance, might act a Control Point for another devices.

E.3.2 Discovery

Devices seek Control Points and Control Points seek devices. A device newly connected to a network advertises the type of Control Point sought, any embedded devices it might contain, the services offered, and a URL to fetch additional information about the device. A device also indicates the approximate length of time it will be available on the network. This expiration provision accommodates mobile devices that join a network for a limited period of time. A device leaves the network at the expiration of the time chosen when the connection was established, or after the device issues a multicast message that it is being disconnected from the network.

A Control Point seeks devices to control using the SSDP protocol (Simple Service Discovery Protocol). Devices to control are located by type and by the services they provide.

E.3.3 Description

Upon acquisition by a Control Point, a device must provide further details about the device type and services offered. The device information is provided by the formal mechanism of Description, which consists of manufacture information and data about each service supported.

Manufacturer information includes model name and number, serial number, manufacturer name and a URL pointing to manufacturer web sites. Each service includes a service type, name, a list of actions and state variables, and URLs. URLs are passed from the device to the Control Point with the locations of service description, control, and eventing data. The Control Point then requests the details using a GET request in the HTTP protocol.

UPnP specifies the format of the data provided by the device to the Control Point in fulfillment of the HTTP GET request. Each device may contain multiple logical devices with Discovery data about each.

The UPnP Forum is specifying templates for the XML language in which devices and services are to be described. Also specified within the XML template are the locations of the URLs pointing to control and event descriptions. An XML service description includes commands to be issued by the device, commands to which the device responds, and associated state variables. The device manufacturer many extend device and service descriptions beyond the template defined by the UPnP Forum.

E.3.4 Presentation

An optional feature allows devices to provide user access for control. The device offers a URL to the Control Point. This URL is made available to the user for accessing with a browser. The user may view the device status and/or control the device according to the intent of the manufacturer. The HTML referenced by the Presentation URL may or may not be related to the control and eventing data. Thus, Presentation may be considered outside the scope of device-to-device communications.

E.4 Control and Event Notification

E.4.1 Communications between Devices and Control Points

A Control Point exercises control over a device by sending a message to the control URL of the device. This message may query the state of a service variable or initiate a service on the device. Similarly, a device may issue a message, called an event, automatically when a state variable changes in a prescribed manner.

Control and event messages, as well as error messages, are formatted using the Simple Object Access Protocol (SOAP). XML structures, called Device Templates, have been specified by the UPnP Forum for a variety of applications including audio/video, lighting, HVAC, and user interfaces. As of October 2004, work is underway on templates for security and energy management.

E.4.2 Control

The following functions are supported for control:

- The Control Point invokes an action on a service supported by a device while passing optional variables.
- The device responds to an action invocation and passes optional output variables.
- The Control Point queries the state of a variable in the device. Each variable must be queried separately.
- The device responds to a Control Point variable query with the current state value. The device is expected to respond within 30 seconds.

E.4.3 Event Notification

The following functions are supported for event management:

- Event subscription: a Control Point subscribes by sending a subscription message to the "Eventing URL" of a device specifying to which service the subscription applies and optionally the duration of the subscription (at least 30 minutes). The location URL to which each event notification is to be sent must be included with the subscription.
- Event subscription initiation: a device acknowledges a new subscription with a unique identifier and the duration of the subscription. Subsequently, the initial states of all subscribed variables are issued by the device. The Control Point can renew a subscription with a request that includes the subscription identifier. Also, the Control Point can cancel a subscription.

Notes on Eventing:

- Subscription to changes in a specific variable is not supported. The service in the device is programmed to specify when a particular variable change is published to the subscribers.
- When any of the specified variables in a service changes, an event message is sent to the subscribers with the present values of the device service variables. The service in a device may be programmed to limit event messages to no more than a specified time interval in the case of a rapidly changing variable.
- Each event message includes an incrementing serial number so the subscribers can determine if an event was missed.

Annex F CEA-851.1, IP-based Telephony (Informative)

F.1 Overview of CEA-851.1

CEA-851.1, "IP-Based Digital Telephony for the Versatile Home Network." defines IP-based telephony for the Versatile Home Network (VHN). Since VHN is an IP-based Internet, it is capable of transporting any IP traffic, regardless of the interpretation of the packet contents. Thus, IP-based telephony transport is "native" to the VHN, and the VHN is transparent to the transport of "telephony" packets. However, as with other services that may be provided using the VHN, control signals for IP telephony require some attention.

Telephony usually implies connectivity to a public telephone network outside the home. Therefore, it will be necessary for the IP telephony end device (which may not be a traditional telephone set) to have a logical interface with software that will probably reside on an access-backbone interface or an access-component interface, such as a Residential Gateway or a cable modem. While it is beyond the scope of CEA-851.1 to specify the architecture or operation of these devices, it is important to require the presence of certain software on the access interfaces.

F.2 Scope of CEA-851.1

CEA-851.1 addresses IP-based digital telephony (sometimes referred to as "Voice over IP") on the VHN. As the VHN is inherently digital, it does not address analog telephony; nor does it address non-packet digital telephony, such as the streaming service provided by ISDN. However, future versions of this standard may address non-IP telephony.

Although this Standard has been issued as a separate document, it is an integral part of CEA-851, "VHN Home Network Specification." Requirements and specifications in CEA-851 also implicitly apply to the functions and devices described in CEA-851.1, unless there specifically stated otherwise.

Annex G - The ISO/IEC 15045 Residential Gateway (Informative)

G.1 Overview of ISO/IEC 15045

In early 2003 work was completed on ISO/IEC 15045 as an international standard for the residential gateway, informally called HomeGate. The HomeGate standard defines the architecture of the residential gateway and a primary set of features.

The function of HomeGate is primarily to translate between a WAN protocol and a LAN protocol. HomeGate includes the following additional features:

- Firewall
- LAN Adapter
- Application Controller

G.2 Firewall

A firewall consists of hardware and/or software that limits what types of messages can flow into and out of the house. The intent of a HomeGate firewall is to provide safety, security, and privacy.

A firewall in a residential gateway allows the user to exercise control over external data entering the house. The user and service provider would agree on specific access rights to deliver purchased services. For example, if there were an agreement for monthly meter readings by a utility, the HomeGate firewall could prohibit daily reads. HomeGate may protect the home network from external attack through address translation and encryption while maintaining connectivity to trusted servers.

Many corporate networks are connected to the public Internet via a processor that inspects data flows to prevent access into the local network from unauthorized or malevolent sources. The HomeGate firewall provides similar privacy management for consumers. HomeGate may be configured to block certain WAN commands that might compromise the safe operation of appliances attached to a home network.

G.3 LAN Adapter

The LAN Adapter feature was developed for home installations without VHN where multiple home network communications protocols are likely to exist. HomeGate accommodates modules called LAN Adapters that translate messages from one home network protocol to another. If the VHN Access-Backbone interface were based on HomeGate, this LAN Adapter feature would not be needed since the VHN backbone carries just one protocol. However, if HomeGate served multiple Access-Component Network interfaces (perhaps with separate plug-in cards), this feature might be a practical alternative to implementing proxies for the component networks to the VHN backbone.

G.4 Application Controller

HomeGate may optionally be a repository for application control functions to support home subsystems such as security, energy management, lighting, etc.

G.5 HomeGate Implementation

An objective of the HomeGate specification is to accommodate this variety of gateways. The simplest gateway connects one WAN to one LAN. A more complex box accommodates multiple WANs and multiple LANs. If multiple gateway boxes are installed, HomeGate specifies methods for these boxes to communicate in order to coordinate service delivery. Multiple gateway boxes may be linked by the LAN, via a private channel, or (less likely) via the WAN, presumably provisioned by the service provider.

The HomeGate standard does not constrain the physical realization of a residential gateway. However, one suggested general-purpose implementation is a box with plug-in cards. The specific set of plug-in cards depends on the WAN and LAN technologies implemented.

G.6 Further HomeGate Developments

[The following is the status as of January 2005.]

HomeGate is a multi-part standard. The first part describing the system architecture is complete and approved. The next part deals with the internal structure of the gateway. Some of these functions include:

- WAN Interface Module
- LAN Interface Module
- Content and control-data flows
- Internal bus
- Internal communications protocol
- Network management