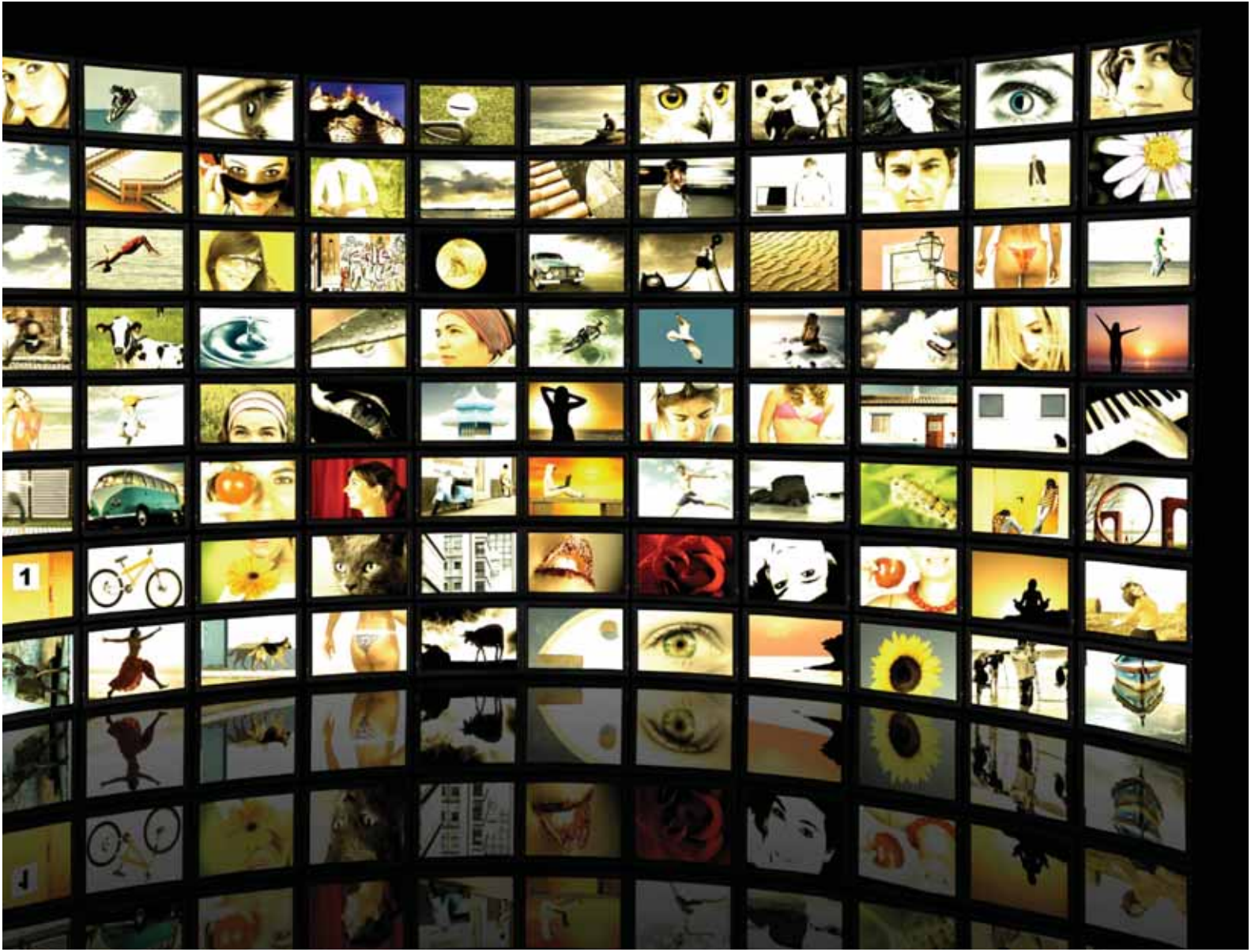


HANA provides a Clear Vision for Home Entertainment

The High Definition Audio-Video Networking Alliance (HANA), takes the lead in setting standards for accessing and sharing high-definition TV content.

This two article series highlights design considerations and solutions HANA presents to address navigation and HD content sharing with an easy to use, single remote control and a single cable through a secure network.





HANA - Reliable Home Entertainment Networking Without the Hassle

By Bill Rose, HANA President

HANA, the High Definition Audio-Video Networking Alliance, is dedicated to ensuring the opportunity function of sharing high definition multi-media entertainment throughout your home is as simple as watching cable TV. With a single remote control you can access content from any HANA device in the home without the hassle of complex set-up menus, network configuration, complex security passwords, or software updates.

Just as importantly, once the content enters the HANA network, whether from the Internet, a cable or satellite provider, or from a DVD player, it may be recorded, moved between devices and even copied freely within the home while remaining completely secure from illegal usage. This is crucial if content owners are to provide their content for download to a home network. This article describes HANA's unified approach to eliminate the problems and shortcomings associated with today's home networks when used to distribute entertainment in a home while providing the content protections necessary to address the security concerns of content and service providers so they will provide the latest movie, TV and music releases to their customers.

Sharing HD Content throughout the Home Currently the only ubiquitous and "consumer friendly" networks in the home for HD movies and TV are the delivery networks - cable, satellite, and the Internet. The problem is, once the content enters the home, it is typically terminated in the receiving device, the settop-box, satellite receiver, or PC where it can only be viewed locally.

There is no simple way to share the content throughout the home or, in the case of the PC, watch it on a TV. The distribution networks found in homes, Ethernet and WiFi, simply do not support sharing HD content in a way that is acceptable to the TV viewing population - the "90%" population that is not tech-savvy.

Addressing the "90%" population requires a new type of network that will support a number of key features unique to entertainment and the viewing habits of the average consumer including:

- **Simplicity** - the "grandma factor"-- anyone, including grandma, should be able to use it
- **Reliability** - no interruptions regardless of what else may be happening on the network
- **Security** - complete protection for the content owner from illegal distribution and copying while remaining essentially invisible to the user
- **Instant Gratification** - Bring it home, plug it in, it works. This means no-new-wires required to share content between rooms, and true Plug-and-Play
- **Standardization** - Any solution must use standardized protocols and technologies to ensure interoperability.

HANA's Solution HANA has one goal that guides everything we do: Keep It Simple - Simple to install, simple to use. We recognize that people watch TV or listen to music for entertainment. Anything that makes it more difficult than watching cable or satellite TV detracts from the experience. Thus HANA took a top down approach beginning with the user's experience and working our way down to the underlying standards that enable the best possible experience for your customers.

Viewing a HANA network from the "10,000 foot" level, it is a Web server/browser architecture allowing HANA browsers, for example a DTV, to connect to HANA servers such as a cable Set Top Box (STB) which will then serve its own menus and graphical user interface (GUI). This is a key point. The TV does not have to understand the nuances of the device it connects to. A five year old DTV does not have to have a driver update to access the latest devices.

To view a program from a STB, the user simply hits a menu key on their remote control and the DTV displays all of the devices connected to the network. Using "Up/Down/Left/Right" arrow keys on the remote, they then select the STB. The DTV then accesses a URL on the STB which serves its Electronic Program Guide (EPG) via HTML to the DTV for display. Again using the arrow keys they can navigate the EPG and select the program to watch. Of course if the STB includes a DVR, they simply can hit the record, pause, fast forward or rewind keys as well, bypassing the menus completely since the DTV

knows which device was selected for viewing and control.

This highlights two features key to HANA's simplicity and reliability. Nothing is simpler than using a single remote control and a few keys to access any device in the home and control all of its functions. And reliability is guaranteed by reserving bandwidth on the network for the duration of the application no matter what else the network is called upon to do. Of course there are many technical details to make this work and that is where we will focus the majority of this article.

Connecting Devices - FireWire™ Makes the Difference

It may seem obvious but if you want a reliable entertainment network, you should start with a network designed to handle entertainment. HANA specifies the use of IEEE-1394 or FireWire™. There are many reasons for this decision including the extensive Quality of Service (QoS) support FireWire™ provides; its ability to operate over many different types of wiring including CAT5 UTP, coax, Plastic and Glass Optical Fiber and others; and its ability to support at least 400 Mbps throughout the home. But the bottom line is that IEEE 1394 was designed from the ground up to support streaming video and audio applications.

FireWire uses a TDMA MAC structure that provides deterministic delivery of data packets allowing applications to reserve bandwidth for as long as it is needed. TDMA or Time Division Multiple Access uses a framed structure that divides the frames into time slots assigning different slots to various applications based on the bandwidth each requires. The number of time slots reserved for a given application is based on the bandwidth needed. Once all of the bandwidth is in use, additional applications are informed that there is no more bandwidth allowing the user to decide if they want to stop another application or wait until it is completed.

Entertainment applications also require tightly controlled latency (delay) and jitter (variation in the time of arrival) of the data to minimize the need for buffering and to simplify system design. To help accomplish this FireWire includes a system clock allowing all connected devices to be synchronized to sub-microsecond levels. This clock is also crucial to ensure audio and video playback is well synchronized and surround sound effects are maintained even when the speakers are connected over the network. To secure content on the network, FireWire uses Digital Transmission Content Protection (DTCP), also known as "5C" for the five Hollywood studios that initially approved it. DTCP has also been approved by CableLabs to protect cable content sent over the FireWire port that is required by the FCC to be on every HD STB. Whenever protected content is moving across the network it is encrypted using the "M6" cipher.

To avoid having content to devices outside the home, the DTLA (the licensing authority for DTCP) also requires a series of messages sent between the source and sink devices that meet a round-trip time of 7 milliseconds.

Finally, FireWire specifies a maximum Bit Error Rate (BER) of 10^{-12} further minimizing system complexity from error handling. Assuming an MPEG2 HD stream of 20 Mbps, a BER of 10^{-12} results in fewer than 1.5 bit errors per 2 hour movie. Contrast this with the 10^{-8} maximum BER specification for Ethernet which could result in nearly 1500 bit errors per movie.

Next Up - IP Networking HANA selected IP as the networking layer for discovery, command and control. While FireWire has its own discovery mechanisms it does not use IP addressing. Therefore HANA also specifies DHCP and Link-Local Addressing (in the absence of a DHCP server) so HANA devices will not only discover other HANA devices, they will be able to discover any IP device on the network. HANA also specifies the use of HTTP and FCP/IP to exchange command and control data again ensuring broad compatibility with other systems. Finally HTML and XML are used to convey the graphical user interface (GUI) between devices. As the languages of choice for Web browsers and servers, this too ensures that HANA devices will easily interoperate with other IP based systems with minimal need for protocol translation.

To support the IP layers discussed above, HANA uses IPv4 Over 1394, RFC 2734. This RFC, approved in 1999, standardizes how IPv4 operates over 1394 networks including Address Resolution Protocol (ARP). The HANA guidelines also reference other IP-based standards such as CEA-2027-B, CEA-931-C and others, providing additional detail as to how the devices will use these IP protocols to achieve interoperability. In particular, CEA-2027-B specifies the Web browser and server used by HANA, the command and control structures and mechanisms, and other details. CEA 931-C defines the AV/C commands defined for 1394 and how they are exchanged on an IP network. Additional protocols such as CSS, DOM, and others are also used in generating the GUI.

No New Wires As noted above, no one wants to buy products only to find out they now need to drill a bunch of holes in their walls to run new wires. HANA, in conjunction with the 1394 Trade Association, has defined a set of standards for bridging IP 1394 over coax cabling. The four part standard is named Networking IEEE 1394 Clusters via UWB¹ over Coaxial Cable and should be approved by the time this article goes to print. Details on the standard will be made available in a white paper released at the time of approval and posted on the 1394 TA's web site www.1394ta.org. Bridges built to this standard will enable an S400 1394 local network (i.e. within the room) to connect to other rooms over the existing coax cabling and through splitters found in most North American homes. It is

designed to coexist with all known signaling found on coax cables today including broadcast cable, DOCSIS modems and Digital Broadcast Satellite (DBS). Simply add a coax bridge to each room where you have 1394 devices, plug the 1394 cables into the bridges, and the coax cable becomes a whole-home 1394 network running at 400 Mbps - fast enough for 5-10 or more HD video streams with bandwidth to spare for other applications.

HANA Content Security While 1394 already supports DTCP to protect content, that is not enough to enable sharing of content between multiple rooms or copying the content for personal use. Content owners are rightly concerned that their HD movies will be "Napsterized" if they are allowed to be networked without "industrial strength" protections. However, most solutions limit the number or type of devices they will operate on.

HANA is developing a new concept in content protection called the Content Cluster. Using broadcast encryption based on AACS (used in Blu-ray DVD players and elsewhere) extended to networked devices, HANA enables content to be "bound" to the home network itself. In effect, your home network appears like a single device.

Once bound to the network, the content may be freely moved around between devices, copied onto hard drives, and even backed up onto optical media. However, once bound to the network, the content is only usable by HANA devices that are members of your network.

If a HANA DVR is removed from the network and added to your neighbor's network, the content will not be usable. This removes the final barrier for consumers. Security is invisible as long as you use the content within your home (or on your own portable devices that are also members of your network).

The content can only be decrypted by a member of the network to which it is bound, and then, only for use on approved outputs such as HDMI and 1394 (using DTCP content protection). It's a win-win: Consumers can finally use their content however they want, while content owners are assured it will not be illegally duplicated or distributed.

Coming full circle, HANA provides everything needed for a home entertainment network; Simplicity - one remote control, one cable; Reliability - using FireWire and its guaranteed QoS; Content Security that is invisible to the user; and the Instant Gratification by turning your existing coax cables into a whole-home network - all based on industry standards.

END

¹ UWB is short for Ultra Wideband.

Next Up-- IP Networking

HANA and DLNA: Why Consumers Need Two Solutions

By Bill Rose, HANA President

Developing a home network is not simple. To be broadly accepted by consumers, manufacturers and service providers, it must operate over existing wiring, protect the high value content being exchanged and connect a wide range of devices and services. The real challenge is to make it simple for home owners to install and use. The Digital Living Network Alliance (DLNA) and the High-Definition Audio-Video Network Alliance (HANA) are both working on home networking solutions that can distribute video entertainment. They both recognize that simplicity is the number one goal. However, the definition of 'simple' in the PC world is not the same as it is for watching a TV.

The Differences DLNA approaches home networking from a PC perspective. Though a PC is not required, the DLNA network was created to solve many of the issues a PC deals with. Those issues have roots in the vast array of devices that come not only from different manufacturers and service providers, but from different industries, each with their own way of doing things. Connecting to these devices requires a set of protocols and device drivers that constantly change with each new generation of devices, processors and operating systems.

Television is a very well defined and unified platform. Cable, satellite and online content providers, as well as CE manufacturers, all come from different industries. However, the rules are already well defined and rarely change. The second difference comes from the ways in which PCs and TVs move data between devices. The PC has traditionally received a file from some source such as the Internet, CD or DVD, and then either used the file itself or moved it to a printer, MP3 player, or other devices to use. The TV operates in a world of real-time streaming. Whether it's over-the-air broadcast, cable, satellite, DVD or PVR, the TV receives an uninterrupted, real time stream

of bits. Any interruption in the stream means an interruption in the viewing or listening experience.

Another difference is in security. We are all aware of PCs' security problems including viruses and hackers. Operating systems and other programs are constantly updated to plug security holes. The potential for a hacked system to allow content theft or illegal copies to be made is a major concern for content owners who zealously protect their products.

Protecting content in a PC environment is extremely difficult and often carries with it many restrictions on usage. The end result has been for most hardware and content providers to use proprietary solutions that only work on their platform, such as Apple TV™, TIVO™, and Netflix™. On closed systems such as TVs, DVD players, or set top boxes, protecting content is far easier than in a PC environment.

Finally, in world of software and firmware updates, consumers are never certain that two devices can work together. Even if they are compatible, issues may arise, due to the ever changing software and device configurations. The TV viewing population can be relatively certain that if something does not work, it's not an incompatibility or missing software issue, but question of correctly connecting and controlling the devices.

With TV having less complex problems, HANA has been able to focus its efforts on creating a standardized solution with one network connection (FireWire™ - the industry name for IEEE 1394), one remote control and one consistent User Interface. (See Why HANA, Why Now for additional information)

Thus it is the starting point – PC versus TV – that defined the problems that HANA and DLNA are attempting to solve and that creates the difference in their definition of 'simple'.

Solutions The PC has evolved to deal with the vast array of different devices and services, by including or downloading the necessary drivers and protocols for each class of device it connects to. In contrast, the TV entertainment system is composed of devices that may never change once they leave the factory. If they are to connect to other devices, the resources needed must be built in from the start.

Both organizations are creating communications methods that will allow devices to communicate over a standard protocol set. However, standardization is, in reality, a negotiation. And since the DLNA's negotiations involved a larger number of companies and industries, each with their own ways of doing things, those negotiations are far more difficult and complex.



In the TV world, the TV and broadcast industries, along with the FCC, have long been the driver for standards. All other devices have been required to accommodate these standards.

Although cable has complicated the situation, the cable, TV and broadcast industries have settled on the codecs (MPEG2, MPEG4, H.264) along with HDMI and the FCC mandated 1394 port for all HD STBs. With the TV specific end of the connection well defined, that leaves only the networking side to complete.

HANA and DLNA utilize many of the same protocols above the MAC and PHY layers (layers 1 and 2). Both are based on IP network protocols. HANA and DLNA use TCP/IP, and either DHCP or Link Local addressing in the absence of a DHCP server. Both also use Simple Service Discovery Protocol (SSDP) to discover devices. With common IP addressing and discovery, devices on a DLNA network are discoverable by those on a HANA network. They also both use XML as a description language and HTTP to transfer information. Furthermore, both use XHTML, a version of HTML that uses XML syntax as their mark up language.

Another similarity is that both organizations require that their specifications be based on public standards. While there are differences, bridging the two should be relatively simple using commonly available software. DLNA requires a larger stack due to its need to communicate with a broader set of devices, but much of the protocol stack is reusable by a HANA device. Finally, HANA devices can operate with a Firefox browser and standard web server software. Since most DLNA networks will include a PC, it is clear that the most common device for bridging the two would be the PC itself.

Quality of Service Moving files versus streaming content place different requirements on the underlying network. For example, a movie is a large collection of bits. Regardless of how those bits are moved, the network has to provide relatively high throughput. The difference is that when moving a file, if some data packets take longer to get through the network, there is little impact on the end user. However, when streaming, delays on the order of milliseconds can create an interruption in the program being watched. The ability to deliver data packets, in a reliable and predictable manner, is called Quality of Service (QoS). Ensuring on time delivery is called guaranteed QoS.

DLNA has selected Ethernet as its primary network, while HANA has selected FireWire™ (IEEE 1394). There are excellent reasons for both choices. Ethernet is the standard network connection for PCs, as well as for broadband modem connections. Ranging from 100 Mbps for 100baseT to 1000 Mbps for gigabit Ethernet, the connection is fast. FireWire has a fast connection as well, with over a billion ports operating at 200

to 800 Mbps today, 1600 Mbps chips now available, and 3200 Mbps on the horizon. While both connections are fast, the basic architecture is very different.

Ethernet is an asynchronous network while FireWire supports both isochronous and asynchronous traffic. This means that Ethernet is inherently built to move files, while FireWire is built to stream. Also inherent in their architecture, is the overhead needed to communicate. The network and processing overhead, generated by adding more network connections, increases rapidly for Ethernet, whereas connecting more devices to a FireWire network only increases the overhead incrementally.

The difference in architecture also affects the approach to QoS. Ethernet was designed as a best effort network. With traditional Ethernet, all devices on the network simply compete with each other to send their data packets. FireWire was designed to guarantee QoS by providing bandwidth reservation. Devices reserve the amount of bandwidth required for as long as it is needed.

The companies developing DLNA are providing several mechanisms that improve Ethernet's QoS. The first is prioritization. Using IEEE 802.1p/q, and UPnP QoS, devices can decide which applications get priority access to the network. While prioritization still does not enable streaming, it does reduce the amount of buffering required at the end device. However, QoS can suffer both unacceptable delays, caused by too many high priority connections being made, and the possibility of lower priority applications not getting through.

UPnP 3.0 specifies a still better solution; parameterization based on work done in IEEE 802.11e and the UPnP Forum. This allows the QoS Manager and QoS Host, as defined in UPnP 3.0, to determine the parameters a connection requires. Such parameters include traffic class and peak, mean and burst data rates, among others. Once these are known, the QoS Manager can negotiate with the QoS Host and allocate the necessary resources to the traffic for a guaranteed connection. UPnP 3.0 also has ways to measure the network performance periodically to ensure it is performing as expected. If a new connection is requested, the QoS Manager determines if the resources exist, and if not, what connections need to be eliminated or limited to free up resources. FireWire does all of this automatically and as such there is no need for QoS Managers and QoS Hosts. The network itself handles the reservations and allocates the bandwidth on a first come, first serve basis. Streaming connections are assigned guaranteed bandwidth on the isochronous channel, those that do not use the asynchronous channel. When there is no more reserved bandwidth to allocate, the requesting service is notified, at which point, the user or a higher layer application can decide how to free up the resources.

While these approaches sound similar, there are a few major differences. The first is that all FireWire devices operate by the same rules – an application requests bandwidth and if the bandwidth is available, it is assigned. If it does not require guaranteed reservations, it is assigned to the asynchronous channel. Ethernet on the other hand cannot truly guarantee a connection. Lower priority applications can be blocked entirely, and even high priority applications can experience non-deterministic latency and jitter.

The network overhead can become particularly problematic. As more data packets are exchanged to provide QoS, the bandwidth available for applications is reduced. There also must be dead time between packets. Therefore as traffic increases, the ability to control latency is reduced. To provide deterministic latency, you must over subscribe bandwidth and limit the size of the packets. This reduces the amount of available bandwidth further. In a typical Ethernet implementation, it is not uncommon to only be able to use 50% of the bandwidth to be assured that video traffic will not suffer delays. For a similarly loaded FireWire network, that number is 90% or more.

Finally, FireWire includes a system wide clock that all devices use. For example, when a video is sent to a TV and the audio to a 5:1 receiver, the two can easily resynchronize to ensure lip sync and maintain surround sound effects. Ethernet has no such clock. Therefore additional protocols (and complication) must be added to resynchronize the data flows.

Ethernet, as the preferred network for the PC, was the logical and obvious network of choice for DLNA. However, that starting point led to a need for additional software and network overhead, in order to support streaming applications. By not worrying about the non-TV applications, HANA is able to specify a simpler protocol stack.

The difference in the choice of MAC/PHY layers and the resulting differences in QoS complicates attempts to bridge the two. However, Pulse-LINK, a fabless semiconductor and HANA member, has developed a technology called CWave™ that simplifies the task. CWave conforms to the 1394 Trade Association's coax bridging standards, specified by HANA for 1394 over coax. When added to a device or coax bridge, CWave delivers 400 Mbps of isochronous and asynchronous over the existing coax infrastructure, without affecting cable or satellite signals. Pulse-LINK is also developing a bridging solution that maps UPnP QoS to the guaranteed QoS provided by FireWire. Thus the coax backbone will ensure that content sent over a local, in-room Ethernet link will be guaranteed the bandwidth it requires between rooms. Therefore CWave can form the backbone for both HANA and DLNA networks.

Security A secure network is critical for high value content. HANA's task is simplified by focusing primarily on closed systems that are inherently difficult to hack. Of course, HANA would like PCs to be able to connect to its network as well. However, the PC is not a central device in a HANA network and most people would forgo connecting it if there are other ways to connect to the Internet.

To secure content, HANA is working with IBM, a HANA member, to develop a new method based on the AACs broadcast encryption used by Blu-ray DVDs. AACs uses AES-128 bit encryption to secure the content. The difference is that AACs is for optical media, not for networks. To extend it to networks, IBM developed ASCCT. ASCCT defines, among other things, a key exchange methodology that allows devices to "bind" to a network to form a cluster of trusted devices. Content that has been legally obtained is also bound to the network. Any bound device will have the necessary information and keys to decrypt bound content for playback. Even portable devices are supported, since as a member of the network, they will have the keys.

In order to obtain a license for the keys, the manufacturer must prove that the keys, and their use to decrypt the content, will occur in a secure processing module. This is typically within a System on Chip (SOC) or a special purpose processor with a secure processing area that is inaccessible from the outside world. Such processors also include methods to ensure the firmware cannot be or has not been compromised in anyway.

A PC is more difficult to secure in this manner. The data paths within the PC, and the processors used, are open to probing using hardware or software. Although possible, it's far more difficult to prove that the keys and content have been and will remain secure. To date, few content providers have been convinced the PC is secure enough for their highest value content such as HD movies.

What's Next? HANA is developing a reference design called The HANA Entertainment Box (or simply THE Box). It connects by Ethernet to any DSL or Cable modem and from there to content service providers. THE Box includes a hard drive to store content and for PVR functionality, the necessary decryption engine and content decoders (MPEG2, MPEG4, H.264) and an HDMI output to a local DTV. It sounds like a DLNA Digital Media Server/Adapter, but that is where the similarities end.

THE Box can also include a FireWire port to connect to cable STBs, which by FCC mandate, must include a FireWire port as well.

STBs already connect to TVs over HDMI, however, THE Box includes a CWave enabled coax jack that can be connected to your existing coax cable infrastructure. The coax connection actually turns every coax jack in the home into a 400 Mbps FireWire network connection. If you want to connect a second DTV in another room, consumers can purchase a HANA Media Client and simply connect it to the coax jack and the HDMI port on the DTV. Thus any DTV can access the Internet, stored content, the cable STB, etc. A single remote control allows you to access and control any connected device using the on-screen graphical user interface.

By using 1394, HANA can utilize the well known and trusted DTCP link protection and localization solution already approved by CableLabs for cable content, the MPAA, and by AACIS for Blu-ray DVD. Combined with ASCCT, the home network becomes a completely trusted environment for even the highest valued content. Once THE Box has been connected to a coax

jack, any HANA device can be connected to the HANA coax network. A typical HANA network based on THE Box can be seen in figure 1.

A benefit of ASCCT security is that a PC can be connected to the network even if it is not secure enough to join the cluster. A content provider can send multi-tiered content to the PC. Standard Definition (SD) content using less secure protection can be viewed on either a PC or a DTV. Higher valued content, such as a recently released HD movie, can be stored as an encrypted file on the PC. The PC would not have the keys and therefore could not decrypt it. It would only be able to stream it over the network to a trusted cluster member, which would have the keys.

Two Solutions For the Home It's clear that consumers would benefit from a simpler PC experience and a simpler TV experience.

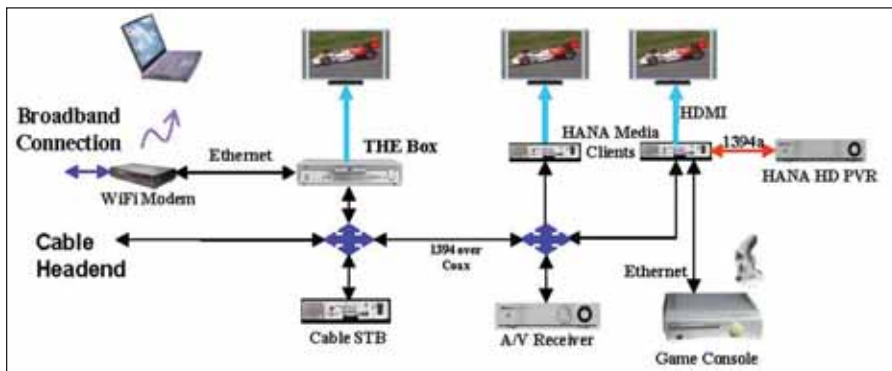


Figure 1: A HANA Home Entertainment Network

HANA will provide the necessary simplicity and reliability expected by consumers when watching TV, regardless of where that program may originate – the Internet, cable or even a PC. DLNA will simplify connecting the vast array of devices consumers attach to their PCs. Consumers will get the best of both worlds by having two separate yet connected networks, each of which is optimized for the task at hand, yet able to share files between them through a bridge, and even across the same 400 Mbps coax backbone.

END

Only Embedded Developer
lets you compare more

than  and  You

can compare  s

And devices and tools.

Then you can buy them. (Wow).

www.embeddeddeveloper.com

One Stop. Shop.

EMBEDDEDDEVELOPER.COM
FIND. COMPARE. BUY.