

Simplifying residential gateway and bridge design

Dr. Eric C. Huang
Vice president of Engineering
Conexant Systems, Inc.

Abstract

The paper shows how engineers can establish a high-performance platform for cost-effective development of a variety of high-speed, Internet-enabled devices that simultaneously support Internet security features, such as virtual private networking (VPN) protection.

The concept of Home Network is explained with brief illustration of different physical network technologies. Then the implementation of residential gateways is described with several switch/router examples, including Ethernet-to-HomePNA, Ethernet-to-HomePlug, and Ethernet-to-Wireless, using a single home-networking processor platform.

Introduction

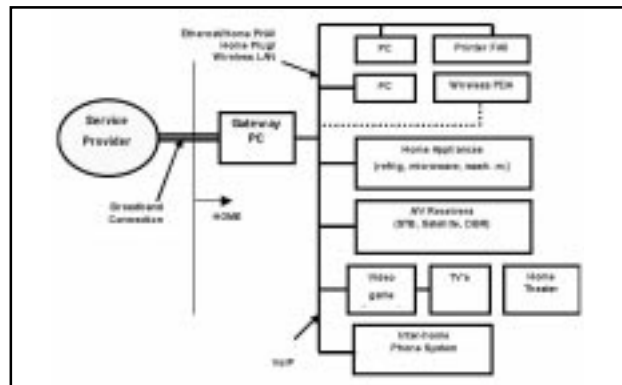
The advent of home networks has propelled the development of Residential Gateways in recent years. Modern home networks have evolved beyond a simple connection network between two or more PC's in the home that was marked by the traditional Local Area Network (LAN). Connecting to external Wide Area Networks (WANs) via a broadband connection such as ADSL and Cable Modem has become essential. Furthermore, additional features such as Network Address Translation (NAT) in the form of a DHCP client, firewall security protection, and different physical connection for the home network, such as the IEEE 802.11b Wireless LAN, Home Plug power line connection, and Home PNA phone line network are becoming necessary.

These requirements have combined to make designing residential gateways challenging. Residential gateways need to include adaptability and flexibility in their designs as well reduced cost and simplicity. They need to adapt to the different possible home network interfaces and have the flexibility to support the myriad of equipment in the home and varying demands for features. The design cost needs to be low, since the products are targeted at the households of the

general population. They also need to be flexible enough to allow for upgrades to Small Office and Home Office (SOHO) environments where more computers are connected and security is of a higher importance. Additionally, in SOHO environments voice communications among different nodes are important tasks to be included in the implementation of the network.

Home network design

The networked home is a product concept that has been on the drawing board of many companies for the past several years. Up till a year ago, home networking remained to mean the connection of two or more computers in order to share external broadband access and peripherals at home. It now includes the connection of entertainment network connection, home control and automation, and even certain type of voice distribution over the data network in the form of packetized voice. It is envisioned by many that this home network is controlled by a Residential Gateway placed between the external broadband and the internal network.



The following diagram depicts how a residential gateway PC is used to channel the data between the external

broadband access network and the internal home network. The home network shown here is multifunctional. It does not only connect the PCs and peripherals, but also controls home appliances, distributes audio/video data through the house, and connects the phones. Residential Gateway design must take into the consideration the physical layer of the home network may utilize many different forms, including Ethernet, phone line, power line, and wireless.

Home network technologies

Because the home network can integrate a number of different technologies, a quick look at what constitutes the physical layer is fundamental to understanding home networks.

Home PNA

Home PNA builds the home network with a technology that utilizes the existing in-home copper wiring in the house for up to 10 Mbps. The technical specification of this technology was developed by the Home Phone Networking Association, hence the name Home PNA. Home PNA is an industry association made up of PC system, networking, and semiconductor companies.

Home PNA data format is based on the Ethernet platform. The Ethernet Media Access Control (MAC) layer data frames are modified so that the HomePNA can be connected to the phone line physical layer. The following diagram shows the difference between the traditional Ethernet data frame and the Home PNA data frame. At transmission, the header of the Ethernet data frame is replaced by data bytes that are specific to phone line wiring. When receiving, the Ethernet data frame is recovered.



Comparison of Ethernet and Home PNA data frames

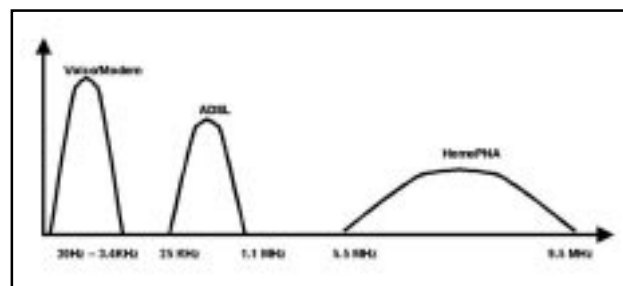
One advantage of Home PNA is that the data transmission can coexist with the voice signal of telephone and ADSL. The Home PNA utilizes the higher bandwidth of the copper wire, while voice and ADSL use lower frequency bands. The following diagram illustrates the sharing of the frequency bandwidth:

Home Plug

Home Plug Power Line Association was formed in April 2000 to develop and promote a high-speed data network using power lines. The physical layer is designed for 10Mbps and uses a technology called Orthogonal Frequency Division Multiplexing (OFDM). OFDM is a method of digital modulation in which a signal is split into several narrow band channels at different frequencies. The technology is focused on minimizing interference among channels close to each other in frequency.

The common challenges of power line data communication include widely varying noise sources, impedance variances, matching problems, multi-path effects, and issues with noise filters originally intended for filtering out

power surges that could pose serious attenuation problems for data signals. Additionally, security among neighboring houses is an issue that needs consideration.



Frequency Sharing of Phoneline

In some respects, OFDM is similar to conventional Frequency-Division Multiplexing (FDM). However, as a contrast to FDM, OFDM gives higher priority to minimizing the crosstalk interference among the narrow band channels as well as the symbols of the data stream, and lower priority to perfecting individual channels. This is ideal for power line based data communication due to the inherent physical problems illustrated above.

Home Plug adopted a collision detection and avoidance scheme called Carrier Sense Multiple Access with Collision Detection (CSMA/CD) which allows data packets to be sent by multiple nodes. When a collision occurs, data packets are automatically resent. Home Plug also implements a prioritization scheme for a basic level QoS (Quality of Service). For security, it uses the 56-bit DES encryption scheme.

Wireless 802.11b

Modern wireless data communications use the 2.4GHz frequency band called the ISM (Industry, Science, and Medical) band in the USA. The following is a table showing the usage of this band in different countries:

Region	Frequency	Bandwidth
Europe	2.4 – 2.4835 GHz	83.5 MHz
France	2.4465 – 2.4835 GHz	37 MHz
Japan	2.4710 – 2.4970 GHz	25 MHz
US	2.4 – 2.4835 GHz	83.5 MHz
Spain	2.445 – 2.475 GHz	30 MHz

The two primary wireless LAN technologies utilizing the 2.4 GHz band are Home RF and IEEE802.11b. Both technologies are based on spread spectrum where carrier frequency is spread over a range. Home RF uses frequency hopping, while 802.11b uses direct sequencing. Direct Sequence Spread Spectrum (DSSS) works by modulating the carrier frequency with a chirp sequence over a fixed frequency band. Frequency Hopping Spread Spectrum (FHSS) allows the signal carrier frequency to hop among several frequency bands. DSSS has a longer range than FHSS, and cells can be more closely grouped together than with FHSS. However, FHSS has better immunity to interferences, especially multi-path interference, lower RF subsystem cost, and

has the capability for more channels (up to 15) to co-locate than DSSS.

802.11b has gained an industry momentum over the past several years and is now the de-facto standard for wireless LAN, with 11-Mbps-data-rate products shipping. As of this paper, it is one of the most suitable and mature technologies for home networking.

Other advanced technologies include 802.11a, which operates at the 5GHz frequency band and can attain a data rate of up to 50 Mbps. However, the RF system is still quite costly and is not yet in the mainstream of products today. The 802.11a uses OFDM modulation to provide superior immunity to multi-path interference.

Residential Gateway (RG)

Residential Gateways can be roughly grouped into the following types: broadband data gateways, entertainment gateways, home automation gateways, and voice/data gateways. The broadband data gateways are designed to allow the multiple PC's at home to share access to an external broadband connection.

In addition to carrying data shared by PC's, an entertainment gateway device also has the functions and features to provide audio and video signal distribution through the house, video play on demand and billing control. An entertainment gateway device has the ability to decode and decompress video signals according to industry standards such as MPEG.

A home automation gateway device allows control of home appliances and the monitoring of home security remotely. A voice gateway adds the feature of packetized voice over the home network media for a multiple attachment phone network. For small offices at home this will eliminate the need for additional phone lines and at the same time make it possible to provide multiple phones.

The functions of residential gateways could include the following:

1. IP address acquisition

Home computers must have an IP address in order to access the public network, corporate network or Internet. It is required for data packets to reach the specific computers. The natural place for assigning IP addresses for home computers is a Residential Gateway.

IP addresses can be static or dynamic. For assigning a dynamic IP address, the RG must support DHCP (Dynamic Host Configuration Protocol) to be either a DHCP server or a relay. As a server, the RG can supply IP addresses to the computers in the home network from a pool of addresses provided by the access network. As a relay, the RG can broadcast the requests from the home network computers to the ISP in the access network to obtain IP addresses. The ISP returns the addresses to the RG, which in turn relays these addresses to the home network computers.

2. Network address translation and firewall

The IP address which a home network computer obtains from either the RG or the ISP in the external access network is usually unique in the domain of either the RG or the ISP. But it may not be globally unique so it must be translated to a unique address. This Network Address Translation (NAT) is performed by the RG. It may also be neces-

sary to translate the port address that identifies a particular IP transaction. This function is called Port Address Translation (PAT) and is also performed by the RG as well. NAT and PAT can implement computer security firewall in its simplest form because they provide a shield on the IP address from the public.

The hiding NAT method hides the IP addresses in the network behind a single IP address and disallows any inbound communication sessions to be initiated from the outside. PAT is similar to hiding NAT in that a single public IP address is used for all private IP addresses. PAT, however, requires that the public IP address be the address of the firewall. NAT/PAT routers do not do much more than hide IP addresses and do not prevent Denial Of Service, or inspect incoming packets.

3. Media translation

The RG needs to translate broadband data to home network. For example, external ATM over ADSL data packets are converted to Ethernet packets in the internal home network. Such translation also involves data buffering and padding when the packet sizes mismatch.

4. Authentication and encryption

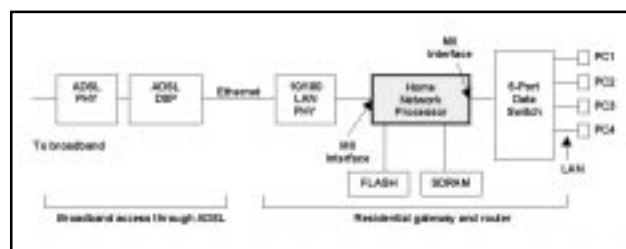
When communicating with the external network, authentication and encryption are usually required by the carrier in order to provide necessary service to the customer. Such functions can be performed by the RG.

For encryption, the Data Encryption Standard (DES) is usually adopted and implemented. DES is an encryption block cipher defined by the U.S. government in 1977 as an official standard. It has a 64-bit block size and uses a 56-bit key during encryption. It is a 16-round Feistel cipher and originally designed at IBM for implementation in hardware. The 3DES algorithm repeats DES three times which makes cracking the encryption extremely difficult.

Residential Gateway Design Using the CX82100 Chip as an Example

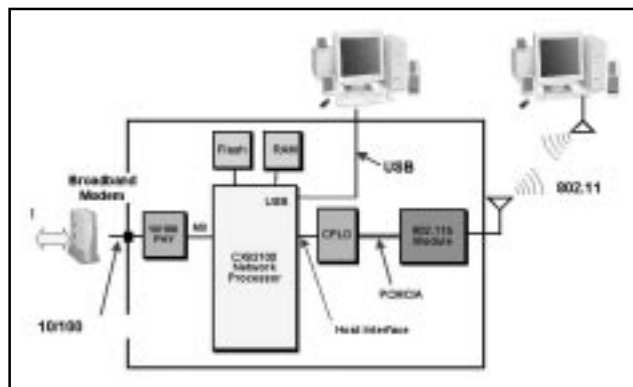
Residential hardware designs employ network processor chips to perform the high level functions mentioned above and physical interface chips to adapt to both the external and internal physical networks. The network processor chips usually include a programmable microcontroller core with embedded software to carry out the different RG functions. This architecture is favored over hard-wired logic because systems feature requirements may change with time. Therefore there is the need for programmability. Also, field upgrades of software are very important. Having a programmable core with the ability to download programs makes field upgrades possible.

The following block diagram gives an illustration of the Residential Gateway design:



In the above diagram, a physical connection chip (PHY), Conexant CX24611, is used to connect to the phone line for Home PNA. The CX24611 chip is designed for the Home PNA 2.0 standard and is capable of 10 Mbps data speed. The connection between the PHY chip and the network processor chip CX82100 is by way of the 7-wire MII (Media Independent Interface).

The following diagram shows how to build a residential gateway to provide an 802.11b wireless home network. The host interface bus of the CX82100 network processor is converted to the PCMCIA standard bus via a CPLD (Configurable Programmable Logic Device). This PCMCIA bus serves as an access point to an 802.11b Module which provides the wireless interface to the computers.



Connection to 802.11b Wireless Home Network

Conclusion

As personal computers and broadband Internet access become more popular, connecting multiple PC's at home and in small home offices becomes necessary. Similarly, the data security of home network is increasingly important. The Residential Gateway device has to provide the functions of broadband access, IP address translation, routing and switching, firewall, and the ability to connect to different physical home networks.

The enabling technology for Residential Gateways lies in a powerful and yet cost-effective network processor that provides a programmable platform. Among other features, the adaptability to different physical home network media and the upgradability to newer and more advanced data communications and security protocols are very important.

About the author

Dr. Eric C. Huang
 Conexant Systems, Inc.
 4311 Jamboree Road, Newport Beach, CA 92660 USA
 Phone: (+1-949) 483 4600
 Fax: (+1-949) 483 7263
 E-mail: eric.huang@conexant.com

Dr. Eric C. Huang is vice president of engineering within Conexant's Personal Computing Division, as well as chair and general manager for Conexant's Communication Technologies Development (CCTD) Co. Ltd. in Shanghai, China. Huang's responsibilities include managing the division's product development in the Greater China area (including China and Taiwan), developing business opportunities for the products developed in the United States and overseeing daily operations of the CCTD.

Prior to joining Conexant, Huang served as director of engineering for Silicon Systems/ Texas Instruments and also as CEO for Sigmax Technology, Inc. Huang's education includes a bachelor's in electrical engineering from National Taiwan University, a master's in electrical engineering from University of California, Los Angeles and a doctorate ABD in computer science from University of California, Los Angeles.