Embedded Information Processors Are Spawning Many Unexpected Applications As They Use LAN and Internet Protocols To Communicate Across Almost Any Network.

Lee Goldberg

INTRODUCTION

1. In today's world, the quantity and variety of network-connected embedded devices are expanding rapidly. The data communication requirements of many of these applications involve frequent query-response or transaction-type exchanges of small chunks of data (small enough to fit into a single, un-fragmented IP packet) between client and server devices. (In this article, "client" refers to the device that initiates such an exchange, and "server" to the device that responds. The client-to-server relationship may be many-to-one, one-to-many, or many-to-many.) In network-connected devices, it is often given that the Internet Protocol (IP) will serve as the network layer protocol. A crucial choice for transaction applications is which protocol to use at the transport layer. In this article, we're going to take a look at several issues and concerns that bear on this choice, especially (but not exclusively) in the context of embedded devices: memory use, network bandwidth, response time, reliability, and interoperability

2. The Remote Device - Internet/Intranet Study is an attempt to connect a Remote machine to the Local/global network of computers known as the Internet/Intranet. This would allow the Remote machine to be controlled from anywhere a connection to the Internet/Intranet could be made. Anyone with a connection to the Internet/Intranet would be able to view the status of the Remote machine. In addition, those with the correct security authorisation would be able to control the Remote machine from anywhere, anytime. Not only would people be able to control the Remote machine from remote locations, but other appliances could also be connected. Knowing that you always enter say a gate from a specified time to a specified time, a computer might open and close the gate for instance (to deter latecomers to work.), or after being informed by the microwave that dinner is nearing completion, a computer might turn the coffee percolator on to provide you with a hot drink to go with your meal. These are all some of the possible scenarios of office/home automation, with each appliance networked together, able to communicate with each other and with other computers elsewhere. This study aims to provide an insight into technology that may one day change the way we live and work.

Remote appliances

3. Over the past decade, devices have become steadily more advanced, and more complicated. This is due in large part to the use of micro-processors to process the user inputs and control the devices. These are known as embedded systems. It is possible to use the micro-processors already inside devices and to add a network connection to allow the appliance to be controlled over the Internet/Intranet.

Fig 1: LG Electronics net enabled washing machine

4. Addition of a micro-processor and some sensors would convert any device into an embedded system. This is easier than developing a complete micro-processor based device, though such devices are readily available in the market today. Hardware and software for connecting an appliance to the Internet/Intranet can then be added, forming a base from which any appliance could be connected to the Internet/Intranet .The advantages of appliances connected to the Internet/Intranet are that through a Graphical User Interface control can be implemented. This makes it extremely simple to control the appliance, and it can be done from any computer connected to the Internet/Intranet. It also makes it possible for other computers or appliances to control the appliance.

AIM OF THE STUDY

5. In order to provide the basics to allow an appliance to be connected to the Internet/Intranet, this study has the following objectives:

(a) For appliances that are connected to the Internet/Intranet to be widely accepted they must be simple and meet several basic requirements.

(b) They must be inexpensive, easy for someone to control remotely, secure and relatively easy to install.

(c) Requiring portable code makes it easy for the code to be modified to run on different processors, if that is desired. Requiring the code to be small in size reduces the amount of memory needed by the processor which also has an effect in reducing the cost of the system.

(d) Two other important considerations are security and privacy. An appliance that anyone can control is undesired as someone might turn the Remote machine on when it is not desired, or turn it off when it is doing some critical job. Some appliances might also keep track of sensitive information, such as if anyone is at home. This information is definitely not in the public domain.

PRODUCT AND TECHNOLOGY REVIEW

6. Here we review the efforts of other individuals and companies in connecting appliances, and other pieces of equipment, to the Internet/Intranet in a variety of different ways using a number of different technologies. A detailed specification of The Remote Device - Internet/Intranet Study and what hardware and software is needed is discussed. It discusses each of the design decisions and why they were made. The Remote Device Internet/Intranet Study which is designed to connect a Remote machine to the Internet/Intranet so that users can access data about the machine, and also control it, remotely. The Paper then presents the objectives of this Study which are to provide the basics in connecting appliances to the Internet/Intranet in an inexpensive and easy manner. Although there are very few commercial appliances available that can be connected to a network or Internet/Intranet, a number of different companies and individuals have connected appliances to the Internet/Intranet as a Study or a product promotion.

The axis neteye 200

7. The Axis NetEye 200 (Figure 1) is one of the first commercially available appliances that can be connected to the Internet/Intranet. It is a camera that can be connected directly to an Ethernet based network, or a modem. This allows it to be placed at a remote location or at an office. The camera contains support for a number of applications used over the Internet/Intranet. These include the Hyper Text Transfer Protocol (HTTP) so that an image can be displayed as part of a web page, and the File Transfer Protocol (FTP) so that a file of a picture can be obtained from the camera. It is also possible to upgrade the software used in the camera by using the File Transfer Protocol.

Figure 1 The Axis NetEye 200

8. A picture is taken whenever an FTP or HTTP request is received by the camera. The picture is then converted into a file, compressed and sent to the requesting machine. The system is based on a 32-bit RISC processor so that the picture can be processed and compressed in a relatively short amount of time. By using already existing applications, it is very easy for anyone connected to the same network or Internet/Intranet to access the camera. This makes the camera very easy to use, but there is little security over who can access the camera beyond limiting the network or Internet/Intranet connection. While this may not be a major consideration with a camera, security is a potential problem when connecting any appliance to the Internet/Intranet.

9. One of the best features of the camera is the ability to upgrade the software from a remote location. This is unusual because those appliances that contain embedded processors do not usually have their software upgraded, they are instead replaced. This improvement is likely to increase the useful lifespan of the product, especially when you consider the enormous growth and change in the Internet/Intranet.

Embedded systems using servers and java applets

10. During the Embedded Systems Conference in Boston in March 1997, the developer 3Soft demonstrated the use of both a Remote machine and a camera that could be controlled over the Internet/Intranet. Both the camera and the Remote machine contained a miniature Hypertext Transfer Protocol (HTTP) server. This made it possible to obtain a web page from both of these appliances that displayed their status. The web pages also contained Java applets that could be used to control the Remote machine and to move the camera around .The use of Java applets has the advantage of using currently available technology, as also providing platform independence. This greatly simplifies the process of actually controlling the appliance. The use of the web interface also means that it uses a system that is in common use across the Internet/Intranet and that is very easy to use.

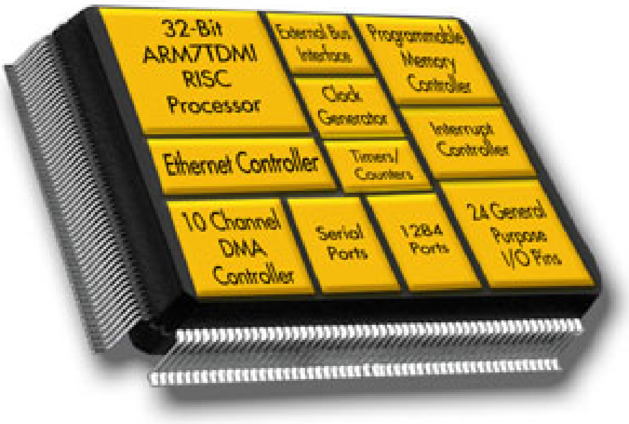
Phar lap weather station

11. This weather station was created by Phar Lap Software as a demonstration of their Micro Web Server, a web page server that supports Java applets and that can create dynamic web pages that change depending on real-time data. It also contains an Operating System developed by Phar Lap. The weather station is based on a 486 Single Board Computer and provides weather data. This is a system that uses already developed applications to provide a graphical interface that can be used to control embedded systems, such as ordinary household appliances.

Network refrigerator

12. The Network Refrigerator consists of a computer with a modem, a microprocessor and a number of sensors. The sensors record the temperature inside the fridge, whether the door is open or not and if there are any cans inside the fridge (and if so, how cold they are). The micro-processor receives the data from the sensors, processes the data so that the computer can understand it and sends the data to the computer. The computer then inserts the data into a web page that can be obtained from its web site While this system does have a large number of different sensors, its main disadvantage is that the micro-processor must communicate through a computer and is not directly connected to the Internet/Intranet. A direct connection to the Internet/Intranet would require fewer components, take up less space and be a lot cheaper.

Net Silicon's Strong arm based solution



13. Net-Silicon's NET+ARM is the ideal platform for developing a network-enabled application. This complete system-on-chip has been thoughtfully designed to balance performance and flexibility. Special features of the NET+ARM solution:

(a) System-on-chip delivers higher reliability, lower unit costs, and smaller footprint

(b) Optimized for cost-sensitive device networking applications

(c) Pre-integrated with board support package, development tools, operating system, networking software, and APIs , Comprehensive technical support and hardware design review services speed your product to production

(d) Powered by ARM, the most popular core in the industry Proven performance in hundreds of network-enabled products worldwide Ideal for Ethernet gateways for serial, wireless, CAN and more .

14. NET+ARM processors form the foundation for the NET+ Works family of integrated hardware and software solutions for device networking. These processors are 32-bit ARM7TDMI-based “system-on-silicon” devices with all of the key functional blocks needed to develop cost-effective, network-connected products. The NET+ARM has been optimized to work efficiently on a 10/100 Base T LAN connection and to move large amounts of data at high speed. This performance is achieved primarily by the unique design of the DMA controller, cache, and bus system which increases effective processor MIPS and system bandwidth. The NET+ARM family ranges from the NET+15, a low-cost processor suitable for network appliance applications to the high performance NET+50. Each of these devices is completely scalable and software compatible, eliminating costly code rewrites and redundancy.

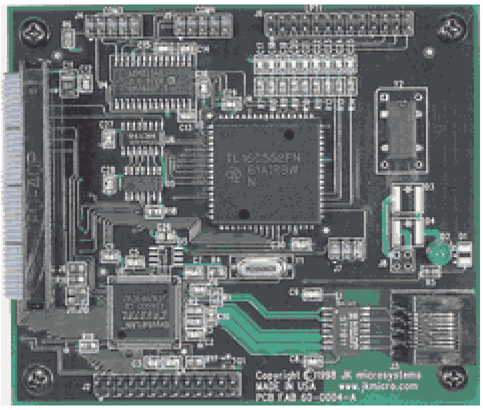
Cambridge university coffee machine

15. This service came into being so that people who were connected to the network at Cambridge University could check to see how much coffee was left in the Vending machine. It consists of a camera that is pointed at the Remote machine and a video capture card inside a computer that obtains a still picture from the camera once every second and stores it as a computer file. The still picture can then be requested by other computers allowing people to check how much coffee is left in the pot. To obtain a picture of the Remote machine from the Internet/Intranet, the web server at the university sends a request to the computer that has the file using a Remote Procedure Call over an ATM network. Although this service consists of a computer that takes a picture of the Remote machine every second, it is an early example of the advantages of on-line appliances. The main disadvantage of the system is the use of two computers, one to obtain the picture and one to act as the web server.

Novell’s embedded systems technology

16. Novell’s Embedded Systems Technology (NEST) is a system that can be used to create networked embedded systems based on a processor. The technology is based on a protocol (known as the NEST Protocol) that provides for a secure and reliable connection with an embedded processor over a network. Remote espresso coffee maker uses the NEST Protocol. This can be implemented using a 286-based board with a 256 kilobyte EPROM along with a programmable Input/Output chip and some logic to control the remote device. As NEST is a commercial product that uses a specialised protocol to communicate with the embedded system, it is necessary to develop a specialised program to control the appliance. This is something of a disadvantage as all of the devices that have already been discussed will run off existing software, such as file transfer or web servers. This does make them easier for more people to use.

Ethernet for flashlite 386 Ex



- **Ethernet**
  IEEE 802.3 Ethernet
  10 MB/sec 10BASE-T
  RJ-45 Connector
  16 bit interface
  Full duplex operation
  Automatic polarity detection/correction
  Packet driver included
  NE2000 Compatible
- **Serial Ports**
  COM3 - wired as DTE
  COM4 - wired as DCE
  RS-232 signal levels
  16C550 High Speed UART
  16 Byte FIFO for each port
  Configurable Interrupts (3,4,5,6)
  115kB maximum speed
- **Parallel port**
  Bi-directional
  DOS compatible as LPT1

17. Flashlite 386Ex controller users requiring local area network connectivity or additional peripherals can utilize the Ethernet/Serial/Parallel expansion board. The board combines a highly integrated, full function, IEEE 802.3 Ethernet controller with 16C550 high speed UARTs (with FIFO) and bi-directional parallel port. The Ethernet port is a 16 bit design that supports a direct connection to 10BASE-T networks, jumper less configuration and internal receive and transmit frame buffers to reduce CPU overhead and maximize throughput. The 2 PC compatible serial ports and the parallel port provide additional I/O necessary for many demanding applications. These features quickly make the Flashlite 386Ex a cost-effective solution for applications such as networking, embedded web and serial protocol conversions. *Ethernet/Serial/Parallel (99-0019)* upgrade kit for Flashlite 386Ex packages the Ethernet/Serial/Parallel peripheral board, interface cables, standoff kit, users manual and schematic to easily convert the unit into the *Flash TCP*. The board is also available without the Ethernet port for users needing to add serial or parallel ports to a Flashlite 386Ex

Intelonet

18. The Embedded Systems Technology that was developed by Novell and described in an earlier section has now been acquired by Intelogis Incorporated, who are also developing hardware to allow a network to be

created by using the existing power lines inside a home or office. The hardware is known as the *InteloNET Power Line* and it makes it possible to create a network by plugging a device into a wall outlet and connecting the other end of the device to the serial or parallel port on a computer. Communication between devices on this network can take place at speeds of up to 1 Mbps. Software is provided that can automatically locate and configure all such devices on the network. The system uses a master/slave architecture where one of the devices is the master while the rest are slaves. This has many advantages in connecting appliances to a network. No additional wires are needed as all communication takes place through the already existing power cord that most appliances possess (unless they run off batteries, of course). The master/slave architecture reduces the amount of processing that needs to be done at the appliance end which in turn reduces the cost of the embedded appliance. If this system were to be used in controlling household appliances then a control unit would be needed (such as a personal computer) to act as the master and to also provide access from the Internet/Intranet (if desired). Whether the computer was the only one with a presence on the Internet/Intranet and all appliances were controlled through it or if each appliance had its own Internet/Intranet address would be largely up to the developer of the system. It should be noted that this technology has major applications in the field of home automation.

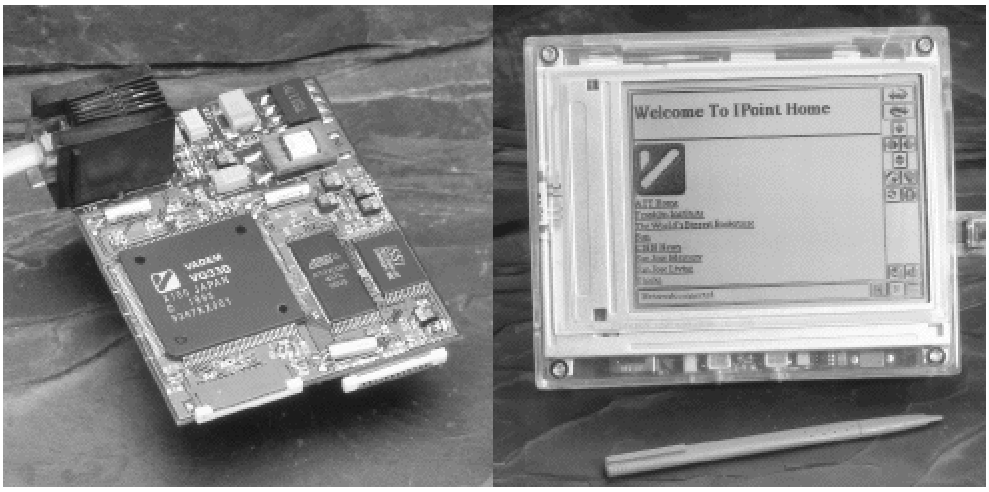
Katix mini-ip

19. This is not an appliance connected to the Internet/Intranet; it is a system that can be used to connect an appliance to the Internet/Intranet. The hardware consists of a microprocessor and an Ethernet controller along with some additional memory. The software consists of a basic operating system and a basic implementation of some of the communication protocols used over the Internet/Intranet. The system is set up as a slave and does not initiate any actions on its own; it only replies to requests from other computers. Although no appliance is connected to this system, the microprocessor used contains many input and output pins that could be connected to sensors used to control an appliance. Unfortunately, no support is given for some of the applications that are in common use over the Internet/Intranet.

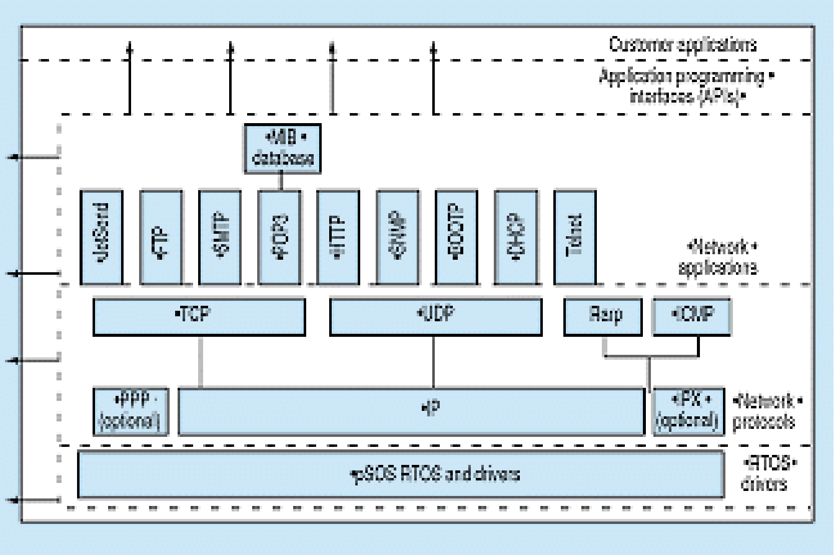
Vadem VG330

20. Embedded systems like the Vadem VG330, a 16-bit, 32-MHz, x86-based, information appliance reference design, can accelerate development of web-enabled applications (a). Integrated with developer's software, the design's I Point firmware handles low-level protocols such as TCP/IP, PPP, and SLIP, plus tasks like modem or ISP setup, and FTP/SMTP transactions. The reference design can be embedded as a standalone Internet interface. With the addition of a display and input device, it can serve as web browser and user interface within a PDA or web-phone. Often, these specialized controllers are bundled with ready-made protocol stacks that speed product development and reduce interoperability problems. In some cases, an even more integrated solution is desirable. For many IA applications, purchasing a

complete reference design or board-level assembly for the communication engine can be a cost-effective choice . Often, these small boards can be purchased and configured for less than the cost of implementing a full-custom communication processor.



In addition to providing all the necessary processing and network interface hardware, these tiny engines also contain embedded firmware with many of the most important protocol stacks (TCP, IP, PPP, UDP, etc.) already in place. The protocols are usually built directly on top of a ROM-based real-time operating system, making user calls from other applications easy and reliable**)**. To further accelerate development, ROM-based network applications like FTP, HTTP, Telnet, POP3, and mail service, as well as the SNMP management functions, can also be provided. These routines are extensively tested and equipped with well-defined APIs.



21. Embedded Internet engines can cut both the cost and development time of information appliances, thanks to their on-chip network interfaces, ROM-based protocol stacks, and network application software. Running under the control of a real-time operating system (RTOS), user applications can simplify mail, file transfer, management, and other well-defined network functions**.**

Motorola Solutions

22. The MC68HC12 is 16 bit micro-processor from Motorola which has a 4 MB address space and an external bus. It also contains chip select signals that reduces the amount of address decoding needed. It can also interface to up to two serial ports. It has a wide range of input and output ports including eight Analog to Digital converters. The MC68HC11K and the MC68HC11A are both 8 bit micro-processors and are part of the 68HC11 family. They both contain a number of different input and output ports including Analog to Digital Converters, Input and Output Compares, Pulse Width Modulation and an interface to a serial port. They also have an external bus and a 64 KB address space. In addition, the MC68HC11K has a paging system that allows the addressing of up to 1MB of memory. It also has a number of chip select signals and a non-multiplexed bus. The MC68HC11A has a multiplexed bus which means that the same lines are used for both addressing and data and a latch is needed to preserve the value of the address being accessed. Ready made boards with requisite ports are available from several manufacturers

DESCRIPTION AND BASIC DESIGN CONSIDERATIONS

23. When designing an appliance that can be controlled from the Internet/Intranet, the first step is to determine what features of the appliance can be controlled and what status information a user might require. If it is for instance a coffee percolator a rather simple appliance, the Remote machine has few controls; it can be turned on or off. Apart from that, the only other things a user can do are add water, add coffee mixture and pour the completed coffee into a mug or cup. The choice of Remote machine will obviously have a bearing on what actions can be easily undertaken by electrical or mechanical equipment. Turning the Remote machine on and off are the two major tasks in controlling a Remote machine. On the other hand, pouring the coffee into a mug when it is finished is unpractical and something best left for coffee drinkers. Adding water and coffee to the machine are both possible, however, the coffee is usually required in a certain section of the machine (such as a filter), making it impractical to allow a remote user to add coffee. Allowing a remote user to add water is more practical, it can be done with a small hose and a valve that can be opened or closed. It is of course necessary to ensure that a remote user cannot overfill the coffee machine. A water level indicator is therefore necessary. This allows the flow of water to be automatically cut-off whenever the water rises above a certain level. Allowing remote users access to the water level indicator allows them to determine if more water is required in the coffee machine. Other useful information that

sensors near the Remote machine can gather are the temperature of the water in the Remote machine, and the current in the wires used to power the Remote machine. This is useful in determining if the Remote machine is operational. If the Remote machine is meant to be on and there is no current in the power lines then something is obviously wrong with the machine there is either a fault or it has been disconnected from the power supply.

24. The only other consideration in controlling the Remote machine is what happens when a local user wants to control it at the same time that a remote user wants to control it. This can be extended to what happens when two remote users want to control the Remote machine at the same time, however this problem can be solved with software. A switch is therefore needed to prevent remote users from using the Remote machine when someone else is controlling the machine locally. Status information about the machine should be able to be obtained, even when remote user control has been disabled.

THE PROCESSOR

25. The processor is the interface between the network and the Remote machine. It relays control information from the network (and locally) to the Remote machine and sensor information back to the network. It contains all the code that is required to control the Remote machine and communicate with the Internet/Intranet. In order to interface with the sensors around the Remote machine, the processor will need a variety of input and output ports. The sensors are generally analog so will require an Analog to Digital Converter. This is because the output of an analog sensor is commonly a variable output voltage. However, a wide range of different ports would be desired for greater flexibility. The processor should also be able to communicate with either a modem or a network. It will also require enough memory to store all programs required that can be run by the processor. This will require additional chips that must be interfaced to the micro-processor which means the bus of the processor must be flexible and easy to access.

THE SOFTWARE

26. In order to be able to communicate with the Internet/Intranet, a number of protocols from the TCP/IP protocol suite must be implemented. A detailed description of the protocol suite can be found at Appendix ‘A’.

Protocols

27. Two application level protocols will be implemented. These are the File Transfer Protocol (FTP), to allow the software on the processor to be upgraded remotely over a network, and the Hyper text Transfer Protocol (HTTP) to allow status information about the Remote machine to be obtained and the Remote machine to be controlled via a web page. This has the advantage of ease of use and no application must be developed in order to

control the Remote machine. Any error information can be provided on the web page that contains the status of the Remote machine. It is also necessary to prevent two remote users from attempting to control the Remote machine simultaneously. This can be accomplished by allowing only one request to the HTTP server at a time and ignoring all others. In other words, the processor will finish servicing one request before servicing a second. This is quite different from most web servers which are capable of servicing many requests at the same time.

28. Other protocols in the TCP/IP protocol suite that should be implemented are those that permit the use of HTTP and FTP over either a network or a modem. The software should also be able to accept inputs from the local controls and determine whether the Remote machine is configured for local or remote control.

Security

29. Another important area of the software is security features. The most important area of security is with FTP when upgrading software. It is vitally important that only authorised people are able to upgrade the software on the Remote machine over a network. This requires the use of a secure login name and password. Some limitations should also be imposed in allowing people to control the Remote machine. While a password or login name is probably necessary, it could limit the interaction by the Internet/Intranet address of the requesting machine. In other words, only computers with an Internet/Intranet address within a certain range would be allowed to control the Remote machine. Limiting who can view the status of the Remote machine is probably unnecessary as simply viewing status information can do little harm to the Remote machine.

OVERVIEW OF DESIGN

30. The design of The Remote Device - Internet/Intranet Study can be done in a top down manner. There are two main sections of the design:

(a). The actual Remote machine and sensors

(b). The controller which contains a micro-processor, a network connection and input and output ports. The controller accepts input from the Remote machine, network, and local controls. It outputs replies to the network, and control signals to the Remote machine. The Remote machine accepts control signals from the controller and relays status information back. Figure 2 illustrates this process.

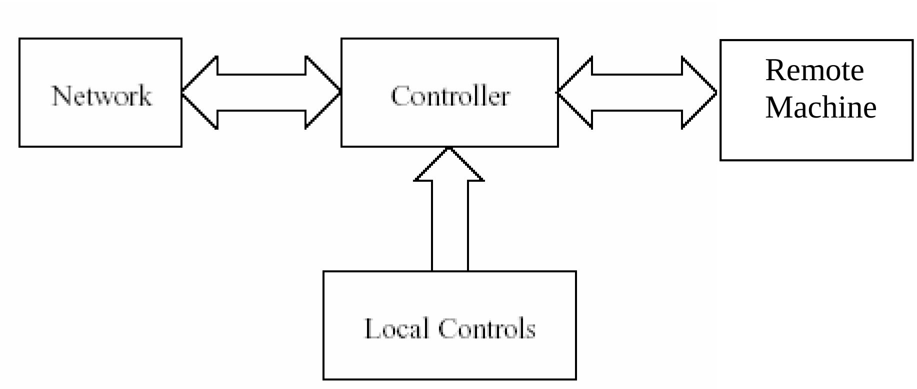


Fig 2 –High level Block Diagram

(c). The local controls consist of switches one to turn the Remote machine on and off and one to select between network control and local control. The network is either a Local Area Network (which may or may not be connected to the Internet) or another computer through a modem connection.

The controller

31. As mentioned earlier, the controller contains a micro-processor, external memory and interfaces to a network or to a modem. The central part of the controller is the micro-processor. A number of different processors were examined for use in this Study, some made by Motorola, AMD, Rabbit, Zilog, VIA and even Intel. It was thought that the use of a broad range of different processors would allow comparisons to be made between them. The processors that were examined include the MC68EN302, the MC68HC16, the MC68HC12, the MC68HC11K and theMC68HC11A from Motorola, Rabbit 2000 and 3000 series based boards,Z-80 CPU based boards from Zilog, Strong Arm based solutions from Net silicon, VIA EDEN Platform and the Intel 8086/80286/80386 based solutions. The MC68EN302 from Motorola is a micro-processor with a built in Ethernet controller. This reduces the number of chips the controller requires and removes the need for interfacing a micro-processor and Ethernet controller.

Software design

32. The device requires the implementation of the TCP/IP protocols that provide for the Hyper Text Transfer Protocol and the File Transfer Protocol over either a network or a modem connection. An important note about the software is that at no time is the Remote machine required to initiate any actions on its own. If a HTTP transfer is required then the requesting machine will send a request, and the Remote machine will generate a reply. When a file transfer is taking place then the computer that is to do the upgrading sends a request to allow data to be sent, while the Remote machine replies with whether the data can be sent or not. Another consideration is that only one HTTP request can be serviced at the same time to prevent clashes when

two remote users try to control the machine at once. Actually, only one HTTP or FTP request can be serviced at once, otherwise problems will arise when the software is being upgraded and someone is trying to access the HTTP server. As both HTTP and FTP use the Transport Control Protocol (TCP) to provide reliable transfer of data, it makes sense to limit TCP to only one connection at a time. This means that only one remote user can access the HTTP or FTP server at once, which also reduces the complexity and size of the TCP code. The servers must also contain the security features for HTTP and FTP that were discussed in the previously.

33. The Internet/Intranet Protocol (IP) must also be implemented, although the need for reassembly of fragments can be avoided through the clever use of TCP. Support for the *ping* program should also be provided as an aid to debugging the system. Since the Remote machine contains an Ethernet controller, a device driver is required to service it, along with the Address Resolution Protocol (ARP) which maps the Internet/Intranet addresses to hardware (Ethernet) addresses. A diagram of the protocols of the TCP/IP suite that must be included can be found in Figure 4.

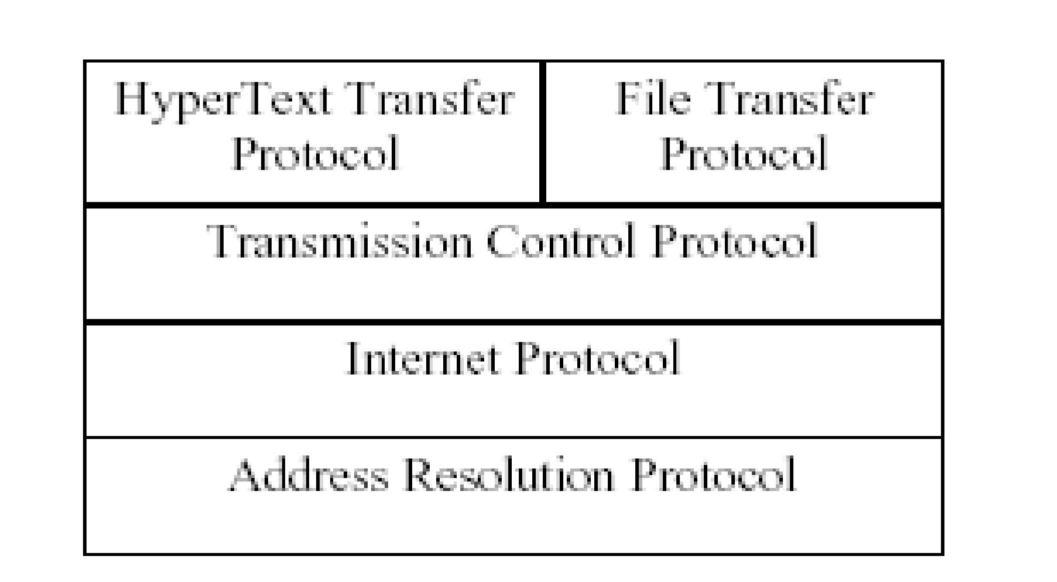

HyperText Transfer Protocol
File Transfer Protocol
Transmission Control Protocol
Internet Protocol
Address Resolution Protocol

Fig 4: TCP/IP Protocol suite

34. Almost all implementations of the TCP/IP protocol suite are done on a machine with an operating system. This is because most of the protocols are implemented as separate processes. An operating system designed for micro-controllers, known as COS was considered but in the end it was decided to implement the software as a series of interrupts. The reason for this is that all the actions performed by the Remote machine are reactions to events. The only time a packet is transmitted over the network is when one is received (which generates an interrupt) and when one is retransmitted (timer interrupt). The local user inputs can all cause interrupts whenever they are changed. This in turn can alter certain global variables that reflect the state of the

machine. The values of the sensors can be stored in global variables inside the micro-processor and they can be updated periodically (using the timer interrupt). Transmission and reception through the serial port are also provided by interrupts. The only major limitation with this system is that small delays might occur in responding to packets when the Remote machine is receiving many requests. This is however unlikely to be a major problem as speed of response is not a major factor with household appliances. The abstraction of the protocol layers can be preserved by the use of procedural calls when receiving incoming packets and to generate replies. In the case of TCP time-out and re-transmission, the packet can be stored in the on-chip memory on the Ethernet controller until it has been acknowledged. To ensure that sufficient memory remains so that packets can be received, only one packet should be waiting for acknowledgment at a time. The next packet can then be sent as a reply to the acknowledgment.

Design of remote controls and sensors

35. Turning the Remote machine on and off can be done through the use of a relay connected to the power supply and an output port on the micro-processor. A five volt output level from the micro-processor can create a closed circuit in the power supply while a zero volt output level from the micro-processor creates an open circuit, disconnecting the Remote machine from its power supply. Measuring the current flowing in the power line can be done by using a rectifier, voltage divider and resistor to obtain the voltage across the resistor. The Analog to Digital Converter can then be used to calculate the current from the resistor value.

EVALUATION OF THE PRODUCT

Advantages

36. Only allowing the Remote machine to service requests dramatically reduces the amount of code that must be implemented in the TCP/IP protocol suite. The decision to allow only one user access to the Remote machine also had an effect on the code by eliminating the need for an operating system. While this allowed much less memory space to be used, it does make upgrading the software for a machine that must be able to initiate actions on its own or respond to multiple requests at once, more difficult. However, for home automation systems it makes sense to utilise the architecture so that there is a central unit or device that is capable of controlling all other connected appliances. In other words, one of the units is the master while all the other appliances are the slaves. This also has the benefit of reducing the software required in the appliances, especially for the very simple appliances such as light switches that should not require much in the way of processing power.

Drawbacks

37. The biggest drawback to the use of the Ethernet network is that a cable is required to link all of the appliances together. This is unlikely to occur in the home for some time to come, if ever, but networked appliances will become popular in industry and office locations where these networks already exist. Embedded networked systems are very useful in that they can provide a Graphical User Interface that can be used to control an embedded system.

CONCLUSION

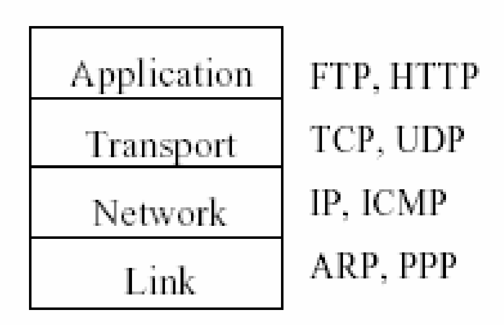
38. It's anybody's guess where these trends will take us, but we can make a few educated prognostications about the near-term outlook. Embedded technologies are making it much easier not only to build intelligence into a product, but also to allow it to communicate with other devices across a variety of infrastructures. This powerful trend will most likely deliver the long-promised "universal information tool," either as a well-connected PDA or a very sophisticated mobile phone. Perhaps the biggest impact however, will be in the invisible realm--meter reading, data capture, and industry automation--which benefits from a steady flow of information. One way or another, we're in for yet another big change in how we relate to information and how information comes to us.

APPENDIX A

A BRIEF DESCRIPTION OF TCP/IP

Introduction

1. The TCP/IP protocol suite forms the basis of all communication over the Internet/Intranet. It allows different computers running different Operating Systems over different types of network to communicate with each other. This is achieved by abstraction. The protocol suite is divided up into several different layers with each layer being responsible for a slightly different function. At least one protocol is implemented in each layer and in some layers a large number of protocols are implemented. The different layers of TCP/IP are shown in Figure 1.



Application	FTP, HTTP
Transport	TCP, UDP
Network	IP, ICMP
Link	ARP, PPP

Figure 1 layers in the TCP/IP Protocol Suite

2. The link layer is responsible for the transmission and reception of the actual data from and to the computer. This is generally over a network such as an Ethernet network or over a modem. This layer is responsible for handling the hardware details of the connection to the Internet/Intranet or network. The network layer controls the movement of information or data between different computers. This includes determining where to send the data, error and control messages. The transport layer provides for the actual data transfer between two different applications on two different computers. It differs from the network layer in that the network layer merely delivers the information to the correct computer while the transport layer is responsible for delivering the information to the correct application. The transport layer can also provide more reliability, depending on which protocol is implemented. The application layer is responsible for the actual user application. This includes electronic mail, remote login, file transfer and the world wide web. When transferring data between applications on two different computers, the application layer would pass the data down to the transport layer which would in turn pass the layer down to the network layer and finally the link layer. The data would eventually reach the second computer and the information would be passed up through the different layers until the application received its data. Each layer would in turn undertake their tasks so that the correct transfer of data takes place. Whenever a layer receives data it needs to send, it appends a header to the front that contains information such as the destination of the data, the source of the data and a checksum for detecting errors. Whenever a layer receives data from the network it removes its corresponding header and forwards the data to the next layer, depending on

the contents of the header. When sending data across a network using TCP/IP it is necessary to know the address of the recipient of the data. This is known as an Internet/Intranet address or an IP address and this is a 32 bit number which is unique for each interface to the Internet/Intranet that a computer has. There are two separate sections to an IP address, the first section identifies the network the computer is on while the second identifies the actual computer

The link layer

3. This discussion will focus on two different protocols: the Address Resolution Protocol (ARP) used in Ethernet networks and the Point to Point Protocol (PPP) used in serial transmissions such as through a modem. On an Ethernet network any computer on the network can communicate to any other computer that connects to the same network. The difficulty lies in that to communicate with any other computer on the network, it is necessary to know that computer's hardware address. This hardware address is different from the IP address discussed earlier which is used by the rest of the TCP/IP protocol suite. The Address Resolution Protocol solves this problem by obtaining a hardware address from a given IP address. It does this by broadcasting a message to every other computer on that network asking for the hardware address of the machine with the given IP address. The destination machine replies with the hardware address and the transfer of information can then take place. Mechanisms such as ARP caching reduce the number of ARP requests that have to be made.

4. The Point to Point Protocol is used by modems and connects only two machines by a serial link. As there are only two computers involved, no resolution of address need be made beyond a simple exchange of IP numbers. This protocol is generally used to allow two separate networks to communicate with each other through a serial link or to connect a single machine at a remote location to a network.

Network layer

5. Central to the network layer is the Internet/Intranet Protocol (IP). It provides an unreliable, connectionless service. This means that no checking is done to ensure that a packet actually reaches it's destination and every packet is treated independently; even packets that are traveling from the same source to the same destination. The main purpose of IP is to forward data to it's correct destination. If the destination is a computer connected to the same network then it can simply send the data directly there. However, if the destination is on a remote network the data must be sent to a gateway. Gateways are responsible for transmitting data from one network to another. Whenever a gateway receives data destined for a directly connected computer, it simply forwards the data to that machine. However, if the destination is remote then it forwards the data to another gateway after consulting a routing table to determine the best route to take.

IP also provides a mechanism for fragmenting large packets of data into several smaller packets and transmitting over the Internet/Intranet or network where they are reassembled. The Internet Control Message Protocol (ICMP) is usually regarded as a part of, or subset of, IP. It is used to send error and control messages that are useful in debugging problems with a network. They also are used if data is sent to a nonexistent network or computer.

Transport layer

6. There are two common transport protocols in use. They are known as the User Datagram Protocol (UDP) and the Transmission Control Protocol (TCP). UDP is simple, not very complicated, but not very reliable. TCP provides for a reliable flow of data between computers and is used by more applications; it is also more complicated as well. Both are similar in that they use port numbers to distinguish between different applications on the one computer. Each packet contains a destination port to specify what application the packet is destined for and a source port that specifies the port to reply to. Common applications such as file transfer have what are known as well known port numbers in that the port number for file transfer is fixed across the entire Internet/Intranet. In addition to the port numbers, UDP only provides an optional check-sum that can be used to check the validity of the data sent. TCP however, provides a reliable method of transmitting data. It does this by several methods. Firstly, before any data is sent, a connection is established between the two computers. Then, whenever any data is sent, an acknowledgment must be received within a certain time or the data is retransmitted. The acknowledgment does not acknowledge the individual packets, rather it acknowledges how many bytes of data have been received. If data must be retransmitted too many times then the connection is closed down. In addition, TCP allows a computer to specify how much data can be received at any one time, thus preventing too much data being sent which results in some of it being lost and having to be retransmitted. TCP also includes a mandatory checksum.

Application layer

7. Although there are a large number of application protocols, only the most common and most useful for an Internet/Intranet appliance are mentioned in this section. The Simple Network Management Protocol (SNMP) is used to access network statistics about a computer and to notify a network manager when a problem occurs in a computer [Stevens 1994]. It is usually based on the UDP transport protocol and could be used by an Internet/Intranet appliance to notify some central authority when a fault or error occurs in an appliance.

8. The HyperText Transfer Protocol (HTTP) is used to obtain web pages and graphics from a remote site. In general, a requests for a web page is received and that page is transmitted back to the requesting machine through the use of TCP where the web browser displays the page on the screen. It could be used by an Internet/Intranet appliance in controlling an appliance.

The File Transfer Protocol (FTP) is similar to HTTP except that the requested file is stored on the hard drive of the receiving machine and the transfer of files can happen in either direction. A file can be transferred to or from a remote computer. FTP is also based on TCP and could be used to update the software on an Internet/Intranet appliance.

9. Simple Mail Transfer Protocol (SMTP) is used for sending and receiving Electronic mail. It is based on TCP and could also be used by an Internet/Intranet appliance to notify a central authority of an error or fault.

The Future of TCP/IP

10. Although the TCP/IP suite has proven its endurance and is likely to be with us for a while, it will undoubtedly undergo some changes. For protocols, as for people, a long life usually requires the ability to adapt to changing conditions. As the Internet continues to grow, the most pressing need is a way to overcome the limitations of the current version of IP in terms of the number of IP addresses available.At the time IP's 32-bit addressing scheme was designed, computers were still expensive devices used primarily by large companies. Many businesses were not yet computerized, and the idea of an individual owning a computer—much less setting up a home network—bordered on absurdity. It must have seemed that there would never be any danger of running out of addresses (and consequently, many usable addresses were "wasted" by the assignment method), but then at that time it was also inconceivable that computers would ever be as powerful and as inexpensive as they are today. When it comes to making predictions about technological progress, the one constant has been a tendency to underestimate. After all, Thomas Watson, former chairman of IBM, is best remembered for the following statement, made in 1949: "*I think there is a world market for maybe five computers*."

Looking Ahead to IPv6

11. IPv6, or IPng (the "ng" stands for "next generation"), is the new version of the Internet Protocol (IP). The Internet Engineering Task Force (IETF) designed it as the next step up from IPv4. It builds on IPv4 and is a natural progression. It is compatible with IPv4, which is currently used on the Internet and other TCP/IP networks. The specific intent of IPv6 is to work efficiently in high-performance networks such as ATM (Asynchronous Transfer Mode), while still working efficiently over low-bandwidth networks (which would include many of the wireless technologies).

Next Generation IP: A Luxury or a Necessity?

12. Why do we need a "next generation" of IP? The answer can be summed up in one word: growth. Internet connectivity has exploded, and it shows no sign of slowing anytime soon. Technology gurus predict that in the future, even our household appliances will be wired to the Internet so we can communicate with them from afar. (This conjures up images of typing in a few

commands and sending them off to your microwave oven, instructing it to have dinner ready when you get home—an idea that may become reality sooner than you think.) If we are to be prepared to assign an IP address to every refrigerator and toaster, we must think big in planning the next version of the protocol that will be used to accomplish these addressing feats. Perhaps the most important lesson to be learned from our experience with IPv4 is that the addressing and routing capabilities of the next generation's Internet Protocol must be able to handle scenarios that may currently seem unlikely, based on seemingly exaggerated estimates of future growth.

Making the Transition

13. Don't worry; it's not likely you'll wake up one day and suddenly see an announcement that on a particular date, at a particular time, the Internet is switching to IPv6. The new version is expected to replace IPv4 gradually, and the two will coexist for a number of years as the transition occurs. Meanwhile, the groundwork is being laid. All Winsock 2.0-compliant applications will automatically support the IPv6 protocol stack. Microsoft is hard at work developing an implementation of IPv6. Cisco is building routers that will take advantage of the next generation of IP.

14. Microsoft Research (MSR) is working on an IPv6 implementation based on the Windows NT/2000 platform. An alpha version of this implementation is publicly available in both source and binary forms. Change is inevitable (except perhaps from vending machines), and network administrators may as well get ready to greet IPv6 with open arms. Like any major transition, there is sure to be some pain involved. The IETF has designed a migration strategy that defines IPv4 and IPv6 as two different protocols with two separate protocol stacks, and IPv6 was designed for compatibility with the older version so the upgrade could be done over time. DNS and DHCP servers will require updating, and the management of coexisting 32-bit and 128-bit addresses is expected to produce some problems. Resistance is futile; the next generation is upon us.

15. The IETF has created a new protocol called 6to4, the purpose of which is to encapsulate IPv6 packets inside IPv4 packets. This will allow networks that migrate to IPv6 early to be able to send their data across the Internet, even if the ISPs they use don't yet support the new version of IP. Many ISPs are now using Network Address Translation (NAT) to allow for the translation of multiple private IP addresses, which don't have to be registered, to a lesser number of public assigned addresses. For this reason, those ISPs have not been in a hurry to implement IPv6 support. Reconfiguring all of their equipment to use IPv6 addresses would be a big project, requiring a great deal of time and effort. The recent popularity of NAT devices and software implementations of NAT (along with inexpensive proxy software) has taken the edge off the urgency of upgrading, at least for some companies. NAT is built into Windows 2000 Server products, and a simple, "lighter" version of NAT called Internet Connection Sharing (ICS) is included in the Windows 2000 and Windows 98SE operating systems. Using one of these, all of the

computers on a network can access the Internet using just one public registered IP address. The new 6to4 protocol will solve the compatibility problem for those corporate networks that do wish to adopt IPv6 sooner rather than later, and may make migration more attractive to others, too. The 6to4 protocol is installed on a router that serves as a gateway from the IPv6 network to the Internet. It works by automatically assigning a prefix to each IPv6 address, which identifies it as a 6to4 address. Then it establishes a tunnel over IPv4, through which the IPv6 packets can travel to another IPv6 network.

Summary

16. In the computer industry, time moves at a pace that's different from the rest of the world. By those standards, the TCP/IP protocol suite has a (relatively) long and venerable history. We can expect it to stay with us for years to come. TCP/IP is *the* protocol stack of the global Internet. Until that changes, its "job security" is assured.

17. But IP must undergo changes to keep up with the extraordinary growth in the number of computers and networks that has been a hallmark of the 1990s, and is expected to continue well into the next millennium. One problem that must be addressed is the very practical one of providing for enough available IP addresses to ensure that we won't run out anytime in the near future. IPv6, the "next generation" of the Internet Protocol, was designed with this goal in mind. It is already being implemented in some quarters, and is likely to enjoy a gradual but steady "takeover" until it finally replaces the current implementation, IPv4. TCP/IP as we know it today consists of an entire suite of protocols. To understand how various protocols in the suite work together, we can use one of the popular networking models as a reference point. Models give us a way to graphically represent and better understand the process of communication between computers that share their resources with one another.

18. The Open Systems Interconnection (OSI) model is the current recognized standard. It was developed by the International Organization for Standardization and provides a set of common specifications to which networking components can be designed. Compliance with the standard ensures that products made by different manufacturers will still be able to interoperate. The Department of Defense (DoD) model is the one on which TCP/IP was originally based. It is an older model, and functions are not as finely divided as in the OSI model, but its layers can easily be mapped to those of the OSI model. Microsoft uses a different model, the Windows networking model, which includes a concept that isn't encountered in the others: boundary layers. Boundary layers are interfaces that are open specifications, and act as "glue" between the component layers of the network operating system software. Understanding the networking models make it easier for administrators to troubleshoot problems with TCP/IP connectivity by helping to narrow down possible sources of the malfunction. The Windows 2000 TCP/IP suite also includes a virtual "toolkit" of utilities, which an

administrator can use to gather information and test connections. The first step in troubleshooting is practicing “preventative medicine”; that is, ensuring that the setup of a new network or the migrating to a new operating system is done in a well-organized fashion. Testing and prototyping, pilot programs, and a thoughtfully planned rollout strategy will go a long way toward reducing the incidence of troubleshooting that will be required later on.

BIBLIOGRAPHY

1. **TTL Cook Book by Don Lancaster**

2. **Microprocessors by Douglas Hall**

3. **Gordon, Daniel; The Trojan Room Coffee Machine;** http://www.cl.cam.ac.uk/coffee/coffee.htm

4. **Haas, Paul; Paul's Extra Refrigerator**; http://hamjudo.com/cgibin/ refridgerator/12456.htm

5. **Intelogis; Intelogis Press Release;** http://www.intelogis.com/press2.htm

6. **Intelogis; Intelogis Press Release;** http://www.intelogis.com/press3.htm

7. **Kintronics; Axis NetEye 200 Features and Benefits;** http://www.kintronics.com/neteye/features.html

8. **Phar Lap; The ETS MicroWeb Server;** http://smallest.pharlap.com/about/microweb.htm

9. **Alhola, Kate; Katix Mini-IP**; http://www.funet.fi/~kate/mini-ip.html

10. **Operating Manual Ethernet to Parallel Adapter** www.sbig.com Email sbig@sbig.com

11. **http://www.communiports.de**

12. **Networking and Telecommunications Fundamentals** www.lucent.com/certification

13. **TROY XCD 10baseT Ethernet Serial Server**

14. **Serial Server Installation Guide For Lantronix MSS1-T and MSS1-T2 Micro Serial Servers and MSS100 Fast Ethernet Micro Serial Servers**.

15. **Some Thoughts on Future Networks**- Tatsuya Suda Professor, University of California (web) netresearch.ics.uci.edu (email) suda@ics.uci.edu

16. Solving noise problems ----------(**ZWorld.com)**
    Rabbit 2000™ Features and Their Use in Board-Level Products
    Interfacing External I/O with Rabbit 2000/3000 Designs
    Rabbit 2000C Release
    Off-the-Shelf Solutions for 802.11b Wireless Networking

Rabbit 2000 Serial Port Software
DeviceMate, an Integrated C Development System for
Network-Enabling Embedded Devices

17. **Parallel Port Complete**
Programming, Interfacing, & Using the PC's Parallel Printer Port
by Jan Axelson

18. **Paraport.net.htm**

19. **http://www.lvr.com/parport.htm**

20. **Microsoft Knowledge Base Article – 154078**
HOWTO Send Raw Data to a Printer Using the Win32 API from Visual Basic.htm

21. **Microsoft Knowledge Base Article – 138594**
HOWTO: Send Raw Data to a Printer by Using the Win32 API

22. **Circuit Cellar- Killing the EMI Demon**

23. **Catalyst Tutorials - An Introduction to TCP-IP Programming**

24. **PC World.com-Surf Among Suds With Web-Enabled Washing Machine**

25. **internet/tcp-ip/tcp-ip-faq/**
tcp-ip-faq@eng.sun.com (Mike Oliver)
http://www.itprc.com/tcpipfaq/default.htm

26. **Dynamic and Mobile VRML Gadgets**
Bastiaan Sch¨onhage and Anton Eli¨ens1

27. **A Taxonomy of Internet Appliances** -Sharon Eisner Gillett and William H. Lehr-Center for Technology, Policy and Industrial Development John T. Wroclawski and David D. Clark Laboratory for Computer Science Internet & Telecoms Convergence Consortium Massachusetts Institute of Technology.
Paper prepared for Telecommunications Policy Research Conference, Alexandria, VA, September 2000

28. **More IP :IP Applications**- Laura Jeanne Knapp IBM Network Consultant 1-919-254-8801 Laura@lauraknapp.com www.lauraknapp.com Thomas M. Hadley IBM Network Consultant 1-919-301-3052 tmhadley@us.ibm.com

29. **Creating the networked home-** Andy Trott, Director of Technology and Strategic Development Dr Paul Entwistle, Head of Technology Pace Micro Technology plc, United Kingdom

30. **iApplianceWeb** - Building secure Internet-centric embedded devices.htm- Gateway lets consumer control home appliances over mobile wireless nets.htm- First Look NetSilicon NET+OS 5 - The first Netcentric Operating Environment.htm- T-TCP enables device to device net transactions.htm- View Under The Hood The Soul Of Ubicom's New 32-bit Internet Gateway Microcontroller.htm

31. Netsilicon, Inc.htm- **NET+ARM® Ethernet-ready System-on-Chip**

32. Information Appliances: From Web Phones To Smart Refrigerators vadem.htm- http://www.digprod.com/.- http://www.sun.com/sparc.- http://www.%20vadem.com/.- http://www.amd.com/.- http://www.digital.com/semiconductor/strongarm/strongar.html.- http://www.lsilogic.com/- mailto:rvgb10@email%20.sps.mot.com; http://www.mot.com/ADC.- http://www.cosystems.com/.- http://www.cybervista.com/.- http://www.gensw.com/.

Comments by Directing Staff

Comments by Head of Department

Comments by Dean FEL