IP ADDRESS PROVISIONING IN A CABLE TV DATA NETWORK

Christopher Grobicki
Director of Product Management
LANcity Cable Modem Division.
Bay Networks Inc.
200 Bulfinch Drive
Andover, MA, 01810 USA
Chris@lancity.com

Abstract. As subscriber penetrations grow in cable TV based networks, the availability of IP addresses for the connected workstations becomes an issue. This paper discusses different methods for assigning IP addresses in this environment as well as upcoming technologies in the TCP/IP networking community that address this issue.

Data communication and information access using the cable TV infrastructure provide cable operators with a new source of revenue at a time when their subscriber base has leveled or started eroding. This new service offering is not available with telephone modems or satellite broadcast services. It features high data rates and application and topology independence. Not only can it prevent existing subscribers from going elsewhere for service, but it can also attract new subscribers. The operator is in a unique position to provide data applications just as varied as the homes and businesses through which the cable passes. These applications can be used to help a community run its businesses, increase productivity, teach its students, help its citizens in occupying their leisure time, and generally, improve the quality of life.

Internet access, work at home, web page cruising and provisioning, and local area network connectivity provide the wide range of applications necessary to interconnect a community to itself and the rest of the world (see Figure 1.)

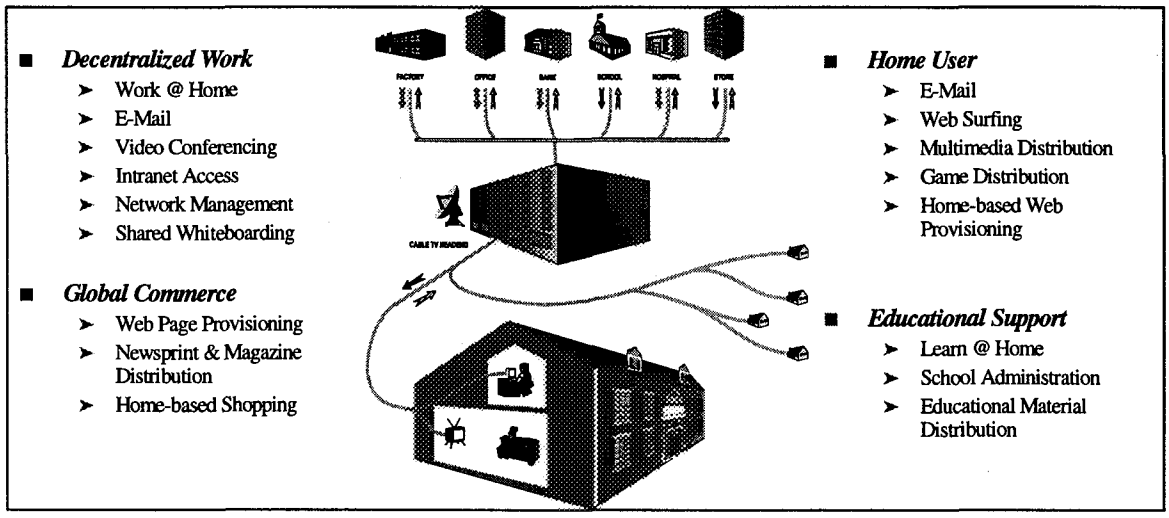

Figure 1. What Data Over Cable TV Enables

TCP/IP has become the standard communication protocol of the Internet, and for seamless connectivity, the cable TV based data network must follow suit. TCP/IP enables worldwide connectivity across the many different physical networks that comprise the Internet. Cable TV is a new addition.

Netscape Navigator and Windows 95 have TCP/IP stacks built into them. Users are asking for services like Web cruising, email, and multimedia distribution. TCP/IP enables these applications.

TCP/IP is more than simply a communication protocol. It provides functionality that allows services to be provided across a neighborhood, town, state, country, and even the world (see Figure 2). A person can communicate with someone in his neighborhood or access a Web site in China, all because of TCP/IP.

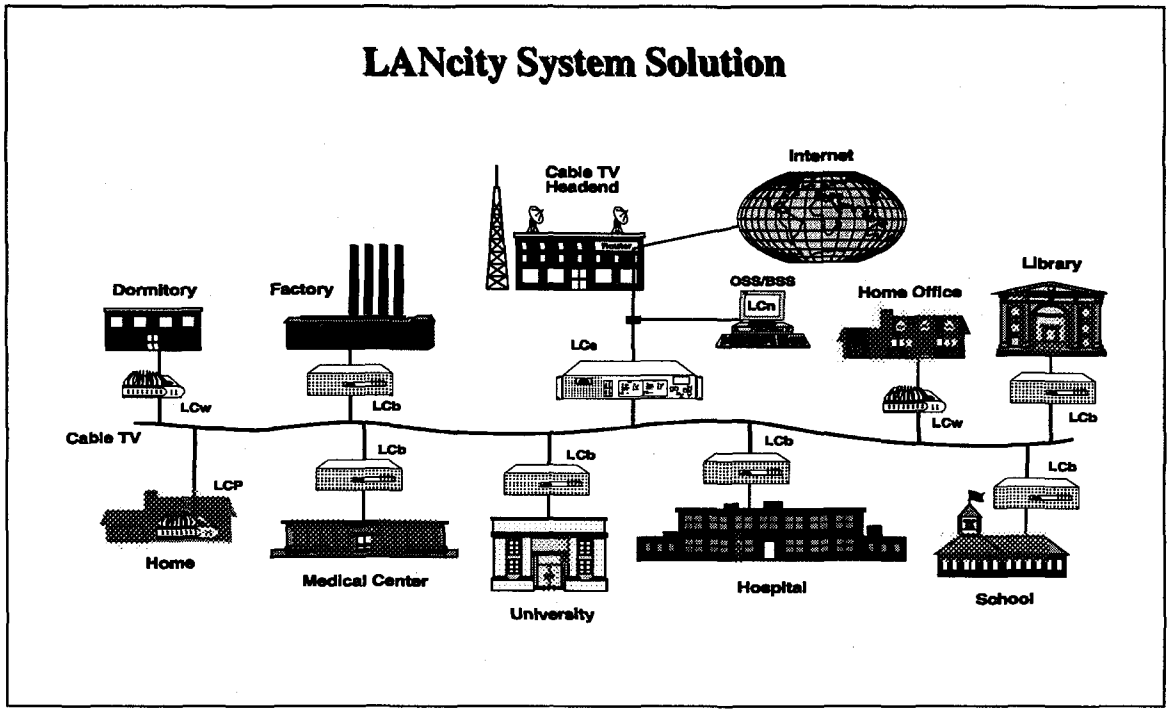

Figure 2. LANcity Solving the Challenges of Data Connectivity

Other communication protocols can provide connectivity for the Internet, but only TCP/IP scales from small networks, isolated to a single building, to very large networks of millions of users. One key reason for the scalability is the elegant addressing structure used in IP. Communication protocols like IPX and Appletalk rely heavily on broadcast addresses to form the basis for intercommunication. While the broadcast function is adequate for Local Area Networks with a small number of PCs, it is much less desirable for metropolitan and wide area networks with potentially millions of users.

While TCP/IP provides an efficient and scaleable choice for large internetworks like the Internet, it also

requires more configurations than are required for small LAN based networks. The network address, host address, the domain name, the subnet mask, the IP address of the routers to get on and off the network, the address of the Domain Name Servers, and additional parameters are required for efficient operation.

These parameters must be programmed into the subscribers' personal computers and workstations before they can access the Internet.

Similar to a person's phone number, which identifies that person in the telephone system, the IP address uniquely identifies a host computing device on the Internet. This address enables information to flow robustly and efficiently from the source to the destination, regardless of whether the path is across town or across the world.

NETWORK ADDRESS HIERARCHY

Data addressing in TCP/IP networks has a hierarchy which provides unambiguous, yet efficient transport of information from one point to another, while isolating the complex layers from the subscriber:

Data Link address: The lowest level address used by a communication protocol to gain access to the local network. Since the Internet is made up of many different types of networks, such as Ethernet at the subscribers home, UniLINK over the cable TV plant, FDDI or ATM for headend interconnectivity, and T1 or T3 for connectivity to the Internet, TCP/IP traffic can traverse many different types of Data Link protocol types, each with their unique addressing scheme. These variables render the Data Link address unsuitable for end to end global communication.

A subscriber should not have to know the Data Link type being used by his communication partner, but because of the different requirements in providing data connectivity in the local, metropolitan, and wide area networks it is impossible to build a universal network from a single hardware technology. Data Link addresses are generally permanently assigned to a communication device and will stay with that device for life. Standardized conventions are used to assure that each communicating device has a unique Data Link address, regardless of where it was manufactured.

IP Address: Internetworking connects many different types of physical networks into a global Internet, providing end to end connectivity without requiring a detailed knowledge of the path traversed. TCP/IP uses the IP address convention to uniquely identify the participants in the global Internet regardless of whether they are connected to an Ethernet, Token Ring, Frame Relay, FDDI or whatever type of network with a global addressing scheme. IP addresses are generally assigned by manual entry or by using an automated and central distribution mechanism which will be described later. IP addresses are not bound to the device nor the user.

Domain Name: Although IP addressing provides unambiguous and compact representations for the source and destination of information flow across the Internet, for a human being

used to dealing with names as opposed to numbers, it can be daunting. In addition IP addresses are not fixed to a subscriber; they can change. Therefore, it is important to incorporate an addressing convention that is easy to administer and understand and yet can remain with the subscriber for life.

The addressing service that satisfies this need is called the Domain Name System (DNS). For example, john.doe@company.com is a syntax that most people Internet users are familiar with. A domain name server administered by the Internet service provider is an efficient, general purpose mechanism for mapping these easy to understand names to the hosts-assigned IP address.

NEED FOR IP ADDRESSES

Unlike AOL and Compuserve, which provide indirect Telco access to the Internet through their server banks, a subscriber to cable TV based data services has direct access to the Internet. This provides the benefit of faster and unlimited access to information, including highly graphical web pages and multimedia applications. Accessing the Internet directly requires the subscriber's PC to become a TCP/IP host on the Internet, thereby requiring an IP address.

The proper administration of IP addresses to the subscriber base is one of the key criteria in providing a reliable and revenue generating service. IP addresses are used not only by applications like Netscape to access the Internet but also in the management of cable modems that use SNMP. This administration can be relatively painless or full of frustration and headaches.

Cable modems that provide a high degree of manageability incorporate an imbedded SNMP agent. This agent standardizes the manner of accessing operational characteristics and provisioning configuration parameters using industry standard management platforms such as HP Openview or Bay Networks Optivity. The SNMP agent requires an IP address to uniquely identify it to the SNMP manager.

CENTRAL ADMINISTRATION OF IP ADDRESSES

There are multiple ways to provision IP address to the subscriber's PC and cable modems. The LANcity Cable Modem Division of Bay Networks encourages the central administration of IP addresses from a server that is under the control of the cable operator or system administrator. This enables better control of the assignments, improves security, and reduces operational maintenance. It is not desirable to "roll a truck" every time a subscriber changes the PC's configuration. Remote reconfiguration is less labor intensive and, therefore, lower cost mechanism.

Three industry accepted mechanisms for the assignment of IP addresses to communication devices are described. The exact method used is determined by the equipment manufacturer's implementation of their products and the cable operator's operational requirements.

Local Assignment: This is the least desirable methodology unless the

number of hosts is small because it requires going to the location the host resides in and manually entering the IP address. If the address changes then another truck roll is required.

BOOTP: A TCP/IP based protocol which provides a static mapping of IP address to the Media Access Control address. It provides a remote mechanism for entering the IP address into a host. This method is simple and robust, ideal for assigning a host with a private IP address that will not be used for accessing the Internet. It is less desirable, however, for public IP addresses which are used to access the Internet because it statically binds them to the Data Link address whether it is actually being used or not. BOOTP is a good allocation protocol for assigning IP addresses to communication devices with SNMP agents because static binding might be desirable to display network configuration maps.

DHCP: BOOTP is slowly being replaced by DHCP which provides the best of all possible worlds. It allows a static mapping of Data Link-to-IP address for management purposes, or a dynamic mapping where the assignment is allocated only during operation or for a specified lease period. This prevents allocating precious IP addresses to workstations not being used and, therefore, allows the address to be reused.

With DHCP a range of IP addresses must be reserved specifically to the DHCP server. If more than one DHCP server exists, each one must be assigned a unique address space.

A knowledgeable Internet Service Provider (ISP) can ease the headaches of IP address and domain name maintenance. Normally ISPs can handle IP address and domain name registration services by working through the proper authorities and agencies, taking over this responsibility from the cable operator.

OVERVIEW OF IP ADDRESSES

The TCP/IP based network, or Internet, is a virtual network built by interconnecting multiple physical networks of different types with routers. Each device on this network must be identifiable with a unique address so that information can traverse from the source to the destination efficiently and robustly. It would be impossible for every router that interconnects the Internet to know where a specific destination address is and know when to forward and when to filter the information. Therefore, something more efficient than a flat address space must be used.

The TCP/IP folks were clever in designing an address that consists of a network address and a host address (see Figure 3).

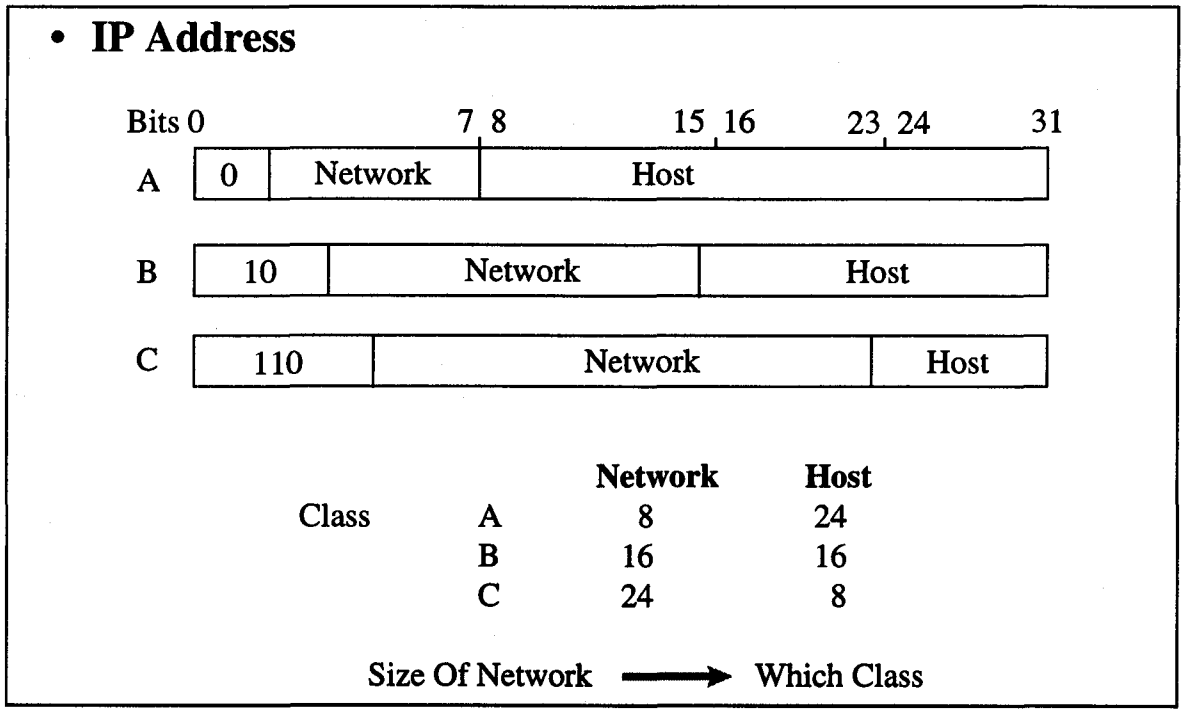

Figure 3. TC/IP - IP Addressing Structure

With this architecture, routers only need to know that they are part of a path to get data they receive to a specific network address and then forward it. Once the packet gets onto the local network, each host looks at the destination address to decide if the packet is destined for it, with all hosts on the network using the same network number.

There are three primary classes of IP network addresses: class A, class B, and class C. Class A addresses allow more than 65,536 hosts, a very large network indeed. These network addresses are assigned to providers like ATT and MCI. Class B addresses are for networks up to 65,000 hosts and are also subscribed to very large users. Class C addresses allow up to 254 hosts and are normally allocated to operators who want to provide Internet services to their subscriber base. Multiple class C addresses can be allocated to a single operator with large numbers of subscribers.

Because the IP address is 32 bits long, it is easy to see that with the explosion of the Internet, network addresses, though still plentiful, must be allocated carefully. Two mechanisms are used to help manage the allocation of class C address space. (Remember, class A , class B, or hard to obtain new service providers are not discussed.) One mechanism is called subnet masking and the other is called supernetting or supernet addressing.

A class C address allows up to 255 hosts on a physical network. What happens when there are fewer than 255 hosts and yet we want to conserve those precious IP addresses? Subnet masking is a standardized, and now required, mechanism that uses the first few bits of

the host address field to specify a local physical network. Because the subnet addresses are derived from the main networks address, subnet masking does not require official assignment since the host addresses belong to the organization with that assigned class C network address.

The administrator, as part of the BOOTP or DHCP address assignment, specifies the subnet mask that indicates what bits are to be used for local network addressing. Therefore, as an example, a single class C address can be divided into two local physical networks that contain up to 126 hosts each.

Supernetting is the opposite of subnet masking but equally important in providing address conservation in a data over cable environment. For example, if fiber legs that are part of an HFC plant extend into multiple neighborhoods, the number of subscribers might be greater than 255, beyond the range of a single class C address. In this case, multiple contiguous class C networks can be joined together to form a single address space, thereby, the allocation of the very precious class B addresses is not required. Classless Interdomain Routing solves the problem of routers needing to understand this concept and collapses a block of contiguous class C addresses into a single router entry specified by the lowest address and a 32 bit mask.

WHERE DO IP ADDRESSES COME FROM?

The network portion of a public IP address is assigned by a central authority to assure its uniqueness. Duplicate IP addresses on the Internet can cause addressing havoc. Therefore, those who access the Internet should follow good procedure to ensure this does not happen.

To get a block or blocks of class C addresses, a network administrator must apply to the Internet Network Information Center in Herndon, Virginia. Class A and B addresses are very hard to obtain and are reserved only for the largest of networks. Class C addresses are assigned in normal situations with contiguous class C addresses assigned for larger networks.

Private IP addresses are used to address IP hosts that do not communicate directly with the Internet. They conserve public IP addresses and yet provide full network connectivity between hosts in an enterprise. In a data over cable architecture, private addresses are used for SNMP management of the cable modems. The address allocation for private internets is specified by Request for Comments (RFC) 1597, issued by the IETF. The addresses fall into the following ranges:

10.0.0.0	to	10.255.255.255
172.16.0.0	to	172.31.255.255
192.168.0.0	to	192.168.255.255

These addresses will never be assigned as public network addresses. Therefore, the use of these addresses does not have to be authorized. The hosts that have these addresses assigned can connect to other hosts inside of the domain but are expected to be filtered out by the routers connecting to the Internet.

The mapping of domain names to IP addresses is handled by the Domain

Name System. Network names at the root level (e.g., lancity.com) must be registered with the NIC to assure uniqueness in naming. The name to the left of lancity.com is administered locally from a DNS server that maps the name to the IP address.

ISSUES WITH IP ADDRESS ASSIGNMENT

Address allocation has come a long way in terms of ease of use. However, the operator must be wary of several pitfalls. Some of these issues exist because of holes in the mechanisms, others because of the distributed, yet public nature of the protocols. The IETF as well as the MCNS organizations are resolving these issues to improve and refine the methodology.

DHCP does not currently support a backup server architecture unless each one has its own IP address space. A backup server is valuable in situations when the primary server crashes and the connected hosts are unable to get their IP address and other parameters for coming online.

Having a backup server prevents this problem but also wastes precious address space. A backup server protocol is being developed to allow backup servers with the same IP address space as the primary server.

Currently, there is no mechanism available that updates IP address changes in a domain name server, thereby requiring a cumbersome manual update to the database. This problem is especially important if one is using the dynamic address provisioning feature of DHCP in a very large network.

Because of the large area of coverage and hard to control subscriber access, security in data over cable networks is a concern and must be addressed.

IP address server spoofing, where an illegal server provisions parameters to the data over cable TV network is being addressed by the cable industry MCNS group.

CONCLUSION

IP address allocation in a data over cable infrastructure is not extremely difficult to understand. However, care must be taken to do it correctly and follow procedures. Otherwise, the service will be hard to maintain and unreliable.

This paper has given a brief overview on the subject. Many excellent TCP/IP texts are available with more details on the subject. Though issues still exist, they are being resolved by multiple organizations that understand the value of robustness and security.