Communications Network Protocols

3.1 Introduction

Previously, we discussed about different architectures and topologies, and how switches and hubs determine where data goes. Most of this discussion was concentrated on how data moves through media and devices. We haven't actually discussed how the devices communicate with each other. For example, to get to Rwanda from Uganda, you can travel by plane or road. Once you arrive in Rwanda, to communicate you either need to speak French, find someone who speaks English, Rwandese or even Luganda, or use an interpreter. The same holds true for networks. All networked devices need a set of rules to follow when they communicate with each other. In this chapter, we discuss these rules.

3.2 Network Protocol

A protocol is a set of rules and conventions that determines how computers exchange information over a network medium. A protocol defines what is going to be communicated. The key elements of protocol are syntax, semantics and timing and may be implemented in hardware or software, or both.

Syntax relates to the structure or format of the data, meaning the order in which they are presented. For example; a simple protocol may expect the first 8 bits of data to be the address of the sender, the second 8 bits to be the address of receiver, and the rest of the stream to be the message itself.

Semantics relates to the meaning of each section of bits. How is a specified pattern going to be interpreted; and what action is to be taken based on that interpretation? For instance does an address identify the route to be taken or the final destination of the message?

Timing refers to two vital characteristics: when data should be sent and how fast they can be sent. For example if a sender produces data at 100 Mbps but the receiver can process data at only 1 Mbps, the transmission will overload the receiver and data will be largely lost.

To effectively manage, support, and maintain a network, you must have a thorough understanding of network protocols and how they operate. Because a protocol determines what language is spoken by the computers on a network, an important decision when designing a network is the choice of protocols. What access is needed and to what types of networks, and whether an interpreter can be used for communicating with networks that speak different languages will all help in determining this. Remember that when you decide on a protocol, consideration must be given to speed, overhead, efficiency, and routing.

Data packets can be sent over the medium using any one of a number of protocols. These protocols are either standard or proprietary. With a standard protocol, users can purchase equipment from any manufacturer because it is programmed to communicate universally. A proprietary protocol is usually protected by patents or other legal stipulations, so users are restricted to purchasing equipment from the developing company or authorized vendors. In a proprietary environment, additional equipment or protocols may be needed in order for the network devices to communicate with devices on standard protocol networks. TCP/IP is considered the language of the Internet and probably the most widely used protocol today hence being referred to as the Universal protocol. Others that fall into this category are; HTTP, SMTP, FTP, Dynamic Host Configuration Protocol (DHCP) etc. The Examples of proprietary protocols are:

- Xerox Network Systems (XNS)
- The Network Basic Input/Output System (NetBIOS)
- The NetBIOS Extended User Interface (NetBEUI)
- Internetwork Packet Exchange/Sequenced Packet Exchange (IPX/SPX)
- AppleTalk- the Macintosh networking protocol
- DECnet – the proprietary network protocol designed by Digital Equipment Corporation.

3.3 The ISO/OSI Model

International Organization for Standardization/Open Systems Interconnection (ISO/OSI) is a set of standards that defines network functionality. The OSI model has been around since 1977. The OSI model is simply a set of protocols which govern the various aspects of networking. This section gives in-depth

information about the various layers of the OSI reference model. ISO/OSI sets standards for cabling, network interface cards (NICs), protocols, and so on. Since the inception of the OSI reference model, the working of internet technology has become very smooth.

The various stages in computer networking can be essentially compiled into the OSI model. Many protocols that correspond to the networking layers reside in the stages of the OSI layers model. A network administrator must know the functions of these protocols so as to have a better understanding of the subject of computer networking. This section will give a fresh perspective on the OSI layers and Ethernet protocols.

Before the advent of the OSI reference model, communication with different entities and different vendors was extremely difficult. This was because every vendor would have a different mechanism to communicate. Therefore, to communicate with entities of different vendors, there arose a need to have a common platform. This need forced the International Organization for Standards to have a viable and universally accepted platform. Thus, the OSI reference model (shown in Figure 3-1) was born.

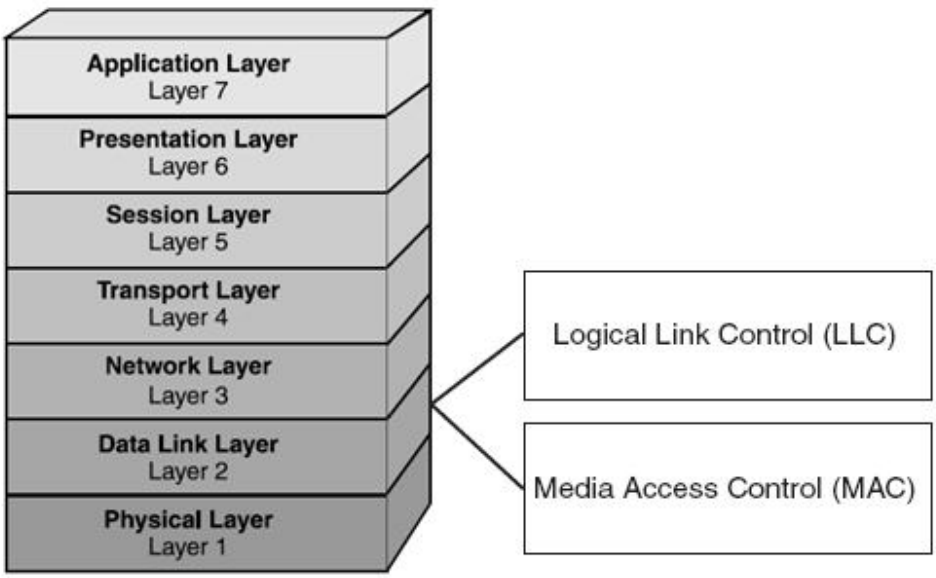

Figure 3-1: The OSI Model

Physical Layer: The physical layer is at the bottom of this data networking model. It deals with crude data that is in the form of electrical signals. The data bits are sent as 0's and 1's. 0's correspond to low voltage signals and 1's correspond to high voltage signals. The mechanical aspects of communication,

such as wires or connectors come under this layer. The physical layer also deals with how these wires, connectors, and voltage electrical signals work. Also, the process that is required for these physical aspects are taken into account in this layer itself.

The Data Link Layer: The Data Link layer provides flow, error control, and synchronization for the Physical layer. It takes information from the Network layer and sends it to the intended device through the Physical layer on the same network. The specifications defined at this layer are network and protocol characteristics. This includes physical addressing, network topology, error notification, sequencing of frames, and flow control. Physical addressing defines how devices are addressed. Network topology determines the specifications that define how devices are to be physically connected. Error notification alerts upper-layer protocols that a transmission error has occurred, and sequencing reorders frames that are transmitted out of order. Flow control monitors the transmission of data so that the receiving device is not overwhelmed with more traffic than it can handle at one time. The IEEE 802.2 specification has divided the Data Link layer into two sub layers: the Logical Link Control (LLC) layer and the Media Access Control (MAC) layer.

The **Logical Link Control** (LLC) layer manages communications between devices over a single link. This includes checking for errors and flow control. The LLC supports both connectionless and connection-oriented services used by higher-layer protocols. Connection-oriented and connectionless communications are discussed later in the "Transport Layer" section. The **Media Access Control** (MAC) sub layer of the Data Link layer manages protocol access to the physical network medium. In other words, the MAC layer controls access and network adapter card drivers. MAC addresses enable multiple devices to uniquely identify one another. These unique addresses are assigned by the manufacturer. Because it only understands the MAC address, this layer cannot route to other networks—it can only pass on packets in its own segment. Devices that operate at this layer are bridges, switches, and routers.

Network Layer: All over the world, there are many different types of networks. These networks are connected to each other through various media. When a data packet wants to reach a particular destination, it has to traverse through these networks. Essentially, there are many operations that are taking place between the connected networks. Also, the packet data which is traversing has to choose an optimum route, and the addressing of these packets

has to be proper. The various operations between the networks, packet data issues, addressing and routing are handled by this network layer.

Transport Layer: The transport layer ensures quality and reliability of the communication. The data packet switching is entirely handled by the transport layer. There are basically two types of packet switching. They are connectionless packet switching and connection oriented packet switching. In connectionless packet switching, the packet data is allowed to choose the route in which it is going to reach the destination. Obviously, the packet in itself cant do this. Physical devices like routers are mainly responsible for the behavior of packets, but the packets formed from the same datum can reach their destination in different ways. Whereas, in connection oriented packet switching, once the route is decided, then all the packets have to follow the same route. Examples of connectionless packet switching are text messages in mobile phones, and the example of connection oriented switching is a direct voice call.

The Sessions Layer: The sessions layer is mainly responsible for creating, maintaining and destroying the communication link. PDU (Protocol Data Unit), in which various protocols are defined, that have to be followed during communication, are the responsibility of the sessions layer. The applications that use RPC's (remote procedure calls) are taken care of by the sessions layer.

Presentation Layer: There are various techniques of data compression which are used to send and receive the optimized data. For example, if certain data is repeating itself for a number of times, then it is logical to send the data only once, and specify the number of times it is repeated. This bundling of the repeated data is one of the techniques of compressions. The compression and decompression of the data is handled by the presentation layer. Also, encryption and decryption techniques used to thwart malicious attacks on data are handled by the presentation layer.

Application Layer: This is the topmost layer of the OSI reference model. This layer comes into picture when there is a process to process communication. Whenever a user invokes any application, all the associated processes are run. Many a times, when an application wants to communicate with another application, then there has to be communication between these associated processes. The application layer is responsible for this interprocess communication.

Since the establishment of the OSI model, there has been a revolution in the field of communication. The entire industry of communication can find its backbone in the OSI reference model. Table 3-1 shows the different protocols that are used at the different layers of the OSI model.

Table 3-1: OSI Layers and the Associated Protocols

OSI Layer	Protocol (s)
Application Layer	DNS, FTP, TFTP, BOOTP, SNMP, SMTP
Presentation Layer	SMB, NCP
Sessions Layer	NETBIOS
Transport Layer	TCP, ARP, RARP, SPX, NWLINK, NETBIOS
Network Layer	IP, ARP, RARP, ICMP, IGMP
Data link Layer	LLC
Physical Layer	LLC

3.4 Transmission Control Protocol/Internet Protocol (TCP/IP)

TCP/IP stands for Transmission Control Protocol/Internet Protocol. It is a set of or suite or stack of small, specialized network protocols, which enable the computers over a network to communicate with each other. TCP/IP is named after the pair of its two most important protocols, TCP and IP. Because of its routing ability, TCP/IP has become the protocol of choice for many LANs as well as the basis for the Internet, making it a standard. TCP/IP is an extensive topic, and there are volumes written on the subject. It is imperative to understand how TCP/IP works as it will be used extensively in routing. If you plan to be a network administrator, you will need some good reference sources on this subject.

A good way to make sense of this is to look at your computer's operating system. Today's operating systems can easily be several gigabytes in size. They include thousands of small files designed to do just one specific task. Separately, they are almost worthless. Together, they form a powerful and comprehensive system that enables your computer to support a seemingly infinite variety of applications. TCP/IP is just like that: lots of little functions designed to do one specific task. Together, they enable your computer to support any type of networked communications activity you would care to do. Before we learn how TCP/IP works, we'll review some history about how it evolved.

3.4.1 A Brief History of TCP/IP

In the early 1970s, the Department of Defense funded the Advanced Research Project Agency (ARPA) at Stanford for research to design a new set of computer communication protocols that would allow multiple packet networks to be interconnected in a flexible and dynamic way. The first phase of this work was successfully completed in July 1977. By 1979, so many researchers were involved in the TCP/IP project that ARPA formed a committee to coordinate and guide the design of the protocols and architecture. This committee was called the Internet Control and Configuration Board (ICCB), and it was active until 1983 when it was reorganized.

The protocol developed was originally called Network Control Protocol (NCP). This success led to the implementation of the two main Internet protocols, Transmission Control Protocol (TCP) and Internet Protocol (IP). By 1980, a serious effort was mounted to require all computers on the ARPANET to adopt TCP/IP. To encourage usage of the new protocols, ARPA made a low-cost implementation available for university researchers. ARPA was able to reach almost all of the university computer science departments in the United States, a feat accomplished in January 1983. Meanwhile, the Internet Architecture Board (IAB) was created from the reorganization of the ICCB. The primary task of the IAB is to set official policies and determine which protocols form the TCP/IP suite.

The success of TCP/IP technology and the Internet among computer science researchers led other groups to adopt it. The National Science Foundation (NSF) realized the importance of computer communication and took an active role in expanding the use of TCP/IP among scientists. In 1985, networks were established around six supercomputer centers. The NSF's interest in high bandwidth was heightened in 1986 through its sponsorship of NSFNET, a new wide-area backbone network. NSFNET gradually reached all the supercomputer centers and tied them to the ARPANET, eventually replacing ARPANET, which was retired in 1990.

In 1992, the U.S. Congress gave the National Science Foundation statutory authority to commercialize the NSFNET.As a result, the Internet Society was created. This is an international organization that encourages participation in the Internet around the world. By 1994, the Internet had reached over 3 million computers in 61 countries. Today, the Internet is growing exponentially, and computers almost everywhere are connected using TCP/IP.

3.4.2 TCP/IP Model Layers Explained

TCP/IP is made up of layers as shown in Figure 3-2 in comparison with the OSI model. Each layer is responsible for a set of computer network related tasks. Every layer provides service to the layer above it. There are in all four layers in the TCP/IP reference model.

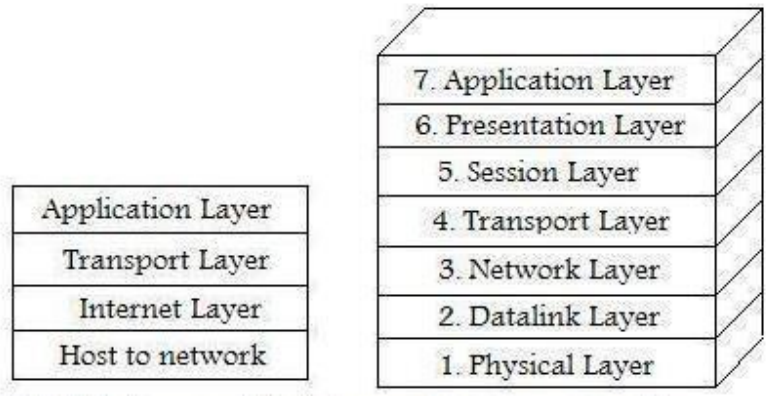

Figure: 3-2: TCP/IP Model Vs OSI Model

- Application Layer: This is the topmost layer of the TCP/IP suite. This is responsible for coding of the packet data.
- Transport layer: This layer monitors end to end path selections of the packets. It also provides service to the application layer.
- Internet Layer: This layer is responsible for sending packets through different networks.
- Link Layer: It is the closest layer to the network hardware. It provides service to Internet layer.

The Transmission Control Protocol operates on the transport layer of the TCP/IP suite and provides the network computers with reliable communication facilities. Email and file transfer are the common applications of TCP. IP, short for Internet Protocol, is a networking protocol used for communicating data over a packet-switched network. It operates on the Internet layer of the protocol suite and facilitates the delivery of datagrams based on the IP addresses of the network hosts. Indeed, TCP/IP protocol suite is the core of communication and computing over the Internet.

Both, TCP/IP model and OSI model, work in very similar fashions. But they do have very subtle differences. Knowing these differences is crucial to learning

computer networking. Table 3-2 highlights the differences between the TCP/IP model and the OSI model.

Table 3-2 TCP/IP Model Vs OSI Model

TCP/IP Model	OSI Model
Defined after the advent of Internet.	Defined before advent of internet.
Service interface and protocols were not clearly distinguished before	Service interface and protocols are clearly distinguished
TCP/IP supports Internetworking	Internetworking not supported
Loosely layered	Strict layering
Protocol Dependant standard	Protocol independent standard
More Credible	Less Credible
TCP reliably delivers packets, IP does not reliably deliver packets	All packets are reliably delivered

3.4.3 Exploring IP Addressing

IP addressing was standardized in 1981, with specifications that required each system attached to the Internet be assigned a unique, 32-bit address value. Systems include servers, routers, gateways, and other networking hardware. A router that attaches two network segments, for example, must have two unique IP addresses, one for each network interface. To ensure that IP addresses used on the Internet are unique, the Internet Network Information Center (InterNIC) must assign any address used on the Internet. InterNIC is the controlling agency for IP addresses and domain names.

3.4.4 Examining an IP address

An IP address identifies the computer or other node (router, printer, server, or other) on the network. Each IP address on a network must be unique. An IP address is a binary number written in a series of four decimal digits, which is known as dotted decimal. Four period-delimited octets consisting of up to 12 numerals forms an IP address. For example, Microsoft's home page IP address is 196.43.133.84 and is a dotted decimal. The numbers represent decimal notations for each of the four bytes of the address; the address identifies the computer. The IP address is really made up of two parts: the network number and the host number.

- The network number identifies the general location of the computer on the network and the host number pins it down to the exact computer. In Microsoft's IP address, 196.43 is the network address.

- The host number is represented by 133.84. Each class of address uses a different manner of dividing the octets. Makerere Univinersity is a Class B network (see the following section).

The highest value in any octet is 255, because of the way the binary format translates to dotted decimal format.

3.4.5 Understanding Address Classes

IP addressing is divided into five categories, or classes. Three of the classes—Class A, Class B, and Class C—are in use today. The following list describes each of the classes:

- Class A is used for large networks. To identify a Class A network address, the first octet uses the numbers from 1 to 126. Class A networks have an 8-bit network prefix; therefore, they are currently referred to as /8s (pronounced “slash eights”) or just “eights.”
- Class B is mainly used for medium-sized networks, and the first octet values range from 128 to 191. Class B network addresses have a 16-bit network prefix; thus, they are referred to as /16s.
- Class C is reserved for smaller networks. To identify a Class C network, the values range from 192 to 233. Class C networks have a 24-bit network prefix, and so are referred to as /24s.
- Class D addresses aren’t used for networks, because they’re special multicast or broadcasting addresses.
- Class E addresses, with values higher than 233 in the first octet, are used only for experimental purposes.

All Class A addresses already have been taken by universities and corporations. Class B addresses are assigned to companies and institutions with a minimum of 4,000 hosts. If you apply for an Internet address, you will probably receive a Class C designation.

Each class defines its own 32-bit address boundaries. In Class C, the first three octets are for the network address; the last octet represents the host address. If you apply for an Internet address, the InterNIC will give you an address with the first three octets defined. You fill in the last octet with numbers ranging from 1 to 254. The numbers 0 and 255 are reserved. Each number you assign

goes to one node on your network, so you can connect up to 254 nodes to the Internet.

3.4.6 Looking at the Subnet Mask

A subnet mask is part of the IP addressing system. A subnet mask creates subnetworks that enable a computer in one network segment to communicate with a computer in another segment of the network. The main reason for subnetting (or creating subnets on a network) is to divide a single Class A, B, or C network into smaller pieces.

The subnet mask is a 32-bit address that hides, or masks, part of the IP address so as to add to the number of computers added to the network. All networks must use a subnet mask, even if they don't connect to another network. If a network isn't divided into subnets, the default subnet mask is used. The default depends on the IP address class.

- Class A networks use a default subnet mask of 255.0.0.0.
- Class B uses a default subnet mask of 255.255.0.0.
- Class C uses a default subnet mask of 255.255.255.0.

Subnetting enables organizations to mix different network technologies across several physical segments. It also enables you to exceed the maximum number of hosts per segment, if you've used all your IP addresses.

3.4.7 Comprehending the Gateway

The gateway is a bridge between two segments of a network. Messages travel between network segments through the gateway. A gateway is a combination of hardware and software; it creates a shared connection between, say, a LAN and a larger network.

Often, you use a gateway to bridge two networks that use different communications protocols. A gateway has its own processor and memory that it uses to convert protocols; converting protocols makes the gateway slower than a router or bridge. A gateway must have its own IP address.

3.7.8 Working with Domain Names

Every IP address on the Internet has a corresponding domain name, such as mak.ac.ug. Domain names make it easy to remember addresses, and you can use them in place of the IP address in the URL text box of your browser.

IP addresses are difficult to remember, so domain names also represent a computer on the Internet. Microsoft's domain name, for example, is www.mak.ac.ug. Domain names usually start with www, which stands for World Wide Web; however, www is not always included in an address. The letters www represent a route to a World Wide Web server.

The second part of the domain name is the name of the organization, company, product, or another catchy word or phrase. mak, for example, is used for the domain name of the Makerere University Web site.

The third part of the domain name identifies the type of organization. The letters com, for example, stand for commercial. Following are other top-level domain identifiers and their meanings:

- gov Government
- mil Military
- net Network providers
- org Nonprofit organization
- edu Education
- ac Academic

Other additions to the domain name include a country code, if the server is located outside of the United States. UK stands for United Kingdom, for example, and IT stands for Italy. Domain names are listed in the Uniform Resource Locator (URL) to a site. The URL is the full address, or computer identifier, on the Web. URLs contain numerous slashes and dots that separate the parts of the address, similarly to the way you separate folders in a path.

Makerere University's complete URL is http://www.mak.ac.ug/ If you want a particular document on a site, you must use a longer URL, such as http://mak.ac.ug/index.php?option=com_content&task=view&id=17&Itemid=71 The letters http stand for Hypertext Transfer Protocol; this is the protocol your computer uses to attach to the server computer. HTTP defines the language the computers will use to transfer pages and hypertext (links). With most new browsers, you don't have to type the http in the address, but it

doesn't hurt to add it. There are no rules as to when to use www or http. The best practice is to copy the exact URL from literature or documentation about the Web site.

3.4.9 Understanding the Domain Name System

The Domain Name System (DNS) is a method of matching IP addresses with domain names. When you type a domain name in the URL address area of your browser, that query is transmitted to a DNS server. A DNS server maintains a database of domain names and IP addresses. The DNS server finds the IP address that matches the domain name and then sends your request on to that server. The process is called name resolution.

You might find a DNS server in a university or college, on a corporate LAN, or even on a smaller LAN. Most primary ISPs also have DNS servers. Local ISPs connect to larger, or secondary, ISPs, and those ISPs connect to much larger, primary ISPs that make up the Internet. DNS, or name, servers are grouped into domains, which identify different levels of authority.

At the top of this hierarchical structure is the root domain, or top-level domain, such as com, edu, org, and so on. Within the top-level domains are second-level domains. Second-level domains contain hosts and subdomains. Going back to the Makerere University example, mak.ac.ug is a second-level domain. A subdomain of mak.ac.ug might be tech. mak.ac.ug. Each Domain Name Server has a specific area for which it stores addresses and domain names. Called the zone of authority, the Domain Name Server can resolve only addresses within its zone. If a Domain Name Server doesn't contain the IP address for the queried domain name, it forwards the query to another Domain Name Server.

3.5 Creating your own TCP/IP Network

When setting up your own TCP/IP network, you need to choose IP addresses for your computers. Remember, each computer on the network needs a unique IP address. You also need to set a specific subnet mask for your network to use.

Several IP addresses are reserved for private use. Following are the three blocks reserved for IP addresses:

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

For your home network, for example, you could use the following IP addresses for five computers on the network:

172.16.0.1
172.16.0.2
172.16.0.3
172.16.0.4
172.16.0.5

Alternatively, you could use the following for your computers:

192.168.0.100
192.168.0.101
192.168.0.102
192.168.0.103
192.168.0.104

You can change numbers only in the last octet of the IP address for a home network or office network. If your corporate network is very large, you can make other changes to the IP addresses, as long as they are consistent. In addition to IP addresses, you need a subnet mask. Use the same subnet mask for all computers on the network. The subnet mask 255.255.255.0 works very well.

3.6 IPv4 and IPv6

IPv4 is 32 bits IP address that we use commonly; it can be 192.168.8.1, 10.3.4.5 or other 32 bits IP addresses. IPv4 can support up to 232 addresses, however the 32 bits IPv4 addresses are finishing to be used in near future, so IPv6 is developed as a replacement.

IPv6 is 128 bits, can support up to 2128 addresses to fulfill future needs with better security and network related features. A primary reason for the new protocol is that the limited supply of 32-bit IPv4 address spaces was being depleted. IPv6 will use a 128-bit address scheme, which provides more IP addresses than did IPv4. IPv6 includes these benefits over IPv4:

- larger address space (128 bits rather than 32 bits)
- simplified header format
- automatic configuration
- more efficient routing

- improved quality of service and security
- compliance with regulatory requirements
- widespread use in global markets

Here are some examples of IPv6 address:

FE80:0000:0000:0000:0202:B3FF:FE1E:8329 This shows a 128-bit address in eight 16-bit blocks.

Here is an example of a collapsed IPv6 address:

FE80::0202:B3FF:FE1E:8329

The :: (consecutive colons) notation can be used to represent four successive 16-bit blocks that contain zeros. When SAS software encounters a collapsed IP address, it reconstitutes the address to the required 128-bit address in eight 16-bit blocks.

Here is an example of an IP address that contains a port number: **[2001:db8:0:1]:80**

The brackets are necessary only if also specifying a port number. Brackets are used to separate the address from the port number. If no port number is used, the brackets can be omitted.

As an alternative, the block that contains a zero can be collapsed. Here is an example: **[2001:db8::1]:80**

Here is an example of an IP address that contains a URL: **http://[2001:db8:0:1]:80**

The http:// prefix specifies a URL. The brackets are necessary only if also specifying a port number. Brackets are used to separate the address from the port number. If no port number is used, the brackets can be omitted.