

Customer Tips

dc00cc0190
January 28, 2004

... for the user

Basic IP Addressing

Purpose

This document presents a basic overview of addressing over the Internet Protocol (IP).

Assumptions

This document is intended for persons who have a rudimentary knowledge of computers, networks and networking terminology.

Open Systems Interconnect (OSI) Model

The Open Systems Interconnect (OSI) model is an ideal framework or construct which networking vendors can use to create or modify communications protocols. A communication protocol is a definition of how devices communicate either directly or over a network. This model can be thought of as a language or formal method of exchanging information.

The OSI model defines several layers of functionality that describe tasks essential to the transfer of information. These layers are represented in Figure 1:

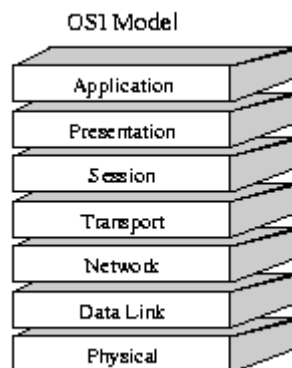


Figure 1

This document applies to these **Xerox** products:

x	WC Pro 32/40 Color
x	WC Pro 65/75/90
x	WC Pro 35/45/55
x	WC M35/M45/M55
x	DC 555/545/535
x	DC 490/480/470/460 ST
x	DC 440/432/425/420 ST
x	DC 340/332 ST
x	DC 265/255/240 ST/LP
x	DC 230/220 ST/LP
x	DCCS 50

- The **Physical Layer** describes the physical properties of the various communications media, as well as the electrical properties and interpretation of the exchanged signals. Example: For Ethernet, this layer defines the type of cable, the type of connector used, and the termination method.
- The **Data Link Layer** describes the logical organization of data bits transmitted on a particular medium. Example: This layer defines the framing, addressing and checksumming of Ethernet packets.

- The **Network Layer** describes how a series of exchanges over various data links can deliver data between any two nodes in a network. Example: This layer defines the addressing and routing structure of the Internet.
- The **Transport Layer** describes the quality and nature of the data delivery. Example: This layer defines if and how retransmissions are used to ensure data delivery.
- The **Session Layer** describes the organization of data sequences larger than the packets handled by lower layers. Example: This layer describes how request and reply packets are paired in a remote procedure call.
- The **Presentation Layer** describes the syntax of data being transferred. Example: This layer describes how floating-point numbers are exchanged between hosts with different math formats.
- The **Application Layer** describes how real work is actually done. Example: This layer implements file system operations.

IP addressing is handled by layer 3, the network layer. IP headers (a portion of a network packet), contain information about the destination and source addresses and other relevant information (such as IP version number, length of the header, checksum, etc.) for a particular exchange of communication.

IP Address Structure

IP addresses are represented in “dotted decimal” notation. For IP Version 4 (the current version most widely implemented, also known as IP V4), the format is as follows:

###.###.###.### ,

Where ### is a decimal number between 0 and 255. Each portion separated by a decimal is referred to as an “octet.” Four octets make up an IP V4 address. In total, 32 bits make up an IP V4 address.

Each address has two basic portions: the **network** address and a **host** address. Think of these as a house number and a street name, where the host address is analogous to the house number, and the network address is analogous to the street name.

The number of bits that make up the network address and the number of bits that represent the host address is determined by the **class** of IP address. There are five classes of IP addresses: A, B, C, D and E. In practice, classes D and E are not used in production environments or on the Internet, and are not discussed here. Classes A, B and C network addresses are assigned as listed below:

IP Address Class	Address Range of First Octet
Class A	1 to 127
Class B	128 to 191
Class C	192 to 223

Hosts that use the Internet must have or show a *public* IP address that is unique. Depending on your country, various agencies assign network addresses for public use. If an organization has host machines that do not access the Internet, then any IP address can be assigned to those machines. These are referred to as *private* addresses.

Subnets

Subnetting is a technique to divide a network to accomplish one of the following:

- Assign and use more network or host addresses than have been assigned to an organization as public addresses. Addresses thus created are not visible on the Internet, and are therefore private addresses.
- You need to divide your site into smaller networks to help reduce traffic, make it more manageable, optimize performance, or span geographical areas.

To accomplish this, *subnet masks* are used. A subnet mask is a 32-bit number that is applied to an IP address to identify the network and node address of a host. Bits

assigned to the network address are assigned a value of 1. Bits that are part of the node address are assigned a value of 0.

For example, a network assigned the subnet mask of 255.255.255.0 for a network address of 132.132.0.0 means that the first three octets of the address designate the *network number*, and the last octet designates the *host address*. This subnet mask allows for 254 networks and 254 hosts per subnet.

A subnet mask of 255.255.254.0 assigns one more bit to host addressing, and one less bit to network addressing. You would have **fewer** network addresses and **more** host addresses available for use than with a subnet mask of 255.255.255.0. This subnet mask allows for 126 subnets and 510 hosts per subnet.

Calculating subnet masks to meet current or future needs (such as to increase the number of network or host addresses, or to manage IP address ranges) may be confusing. Use a spreadsheet or special application to help with these calculations. You can download various shareware or freeware programs from the Internet for this purpose.

The formula for calculating the number of possible subnets and hosts is as follows:

$$\text{Possible subnets} = 2^{(\text{number of masked bits})} - 2$$

$$\text{Possible Hosts per subnet} = 2^{(\text{number of unmasked bits})} - 2$$

For example, a subnet mask of 255.255.252.0 for a the Class B network of 140, uses 6 bits as mask bits. Thus the calculation is:

$$\# \text{ of subnets} = 2^{(6)} - 2 = 62$$

$$\# \text{ of hosts} = 2^{(10)} - 2 = 1022$$

Special IP Addresses

The following addresses have special functions. Do not use these addresses when assigning addresses to hosts:

Address	Function
The network 0.	The default route - used to simplify IP routing tables.
127.0.0.0	Loopback - the address 127.0.0.1 is often used to refer to the local host. Using this address, applications can address a host as if it were a remote host without relying on any configuration information.
Address with all network bits set to 0.	Refers to "this" network.
Address with all host bits set to 0.	Refers to the network itself. For example, the address of 132.132.1.0 refers to network 132.132.1. This notation is used in routing tables.
An address with all bits to 1.	Refers to all hosts.
255.255.255.255	Broadcast.

Broadcast and Gateway Addresses

Host addresses of 255 are reserved for broadcast messages. Each network is also configured with a gateway address, which allows traffic to be directed to other network segments.

Assigning and Acquiring IP Addresses

IP addresses can be either explicitly assigned by an administrator, or acquired from a server when a host attaches to a network.

Assigning IP addresses assumes that the person making the assignment has a full understanding of IP addressing, the architecture of the network with regard to routing capabilities, and other requirements such as growth of the network.

BOOTP (bootstrap protocol) and DHCP (Dynamic Host Configuration Protocol) are two protocols that automatically assign IP addresses to hosts as the hosts attach to the network. While BOOTP and DHCP both need to be managed, they reduce the amount of effort required to manage IP addresses.

A Xerox Multifunction Device and IP Addressing

All Xerox multifunction devices can have IP addresses explicitly assigned by an administrator. In addition, you can configure all Document Centres and WorkCentres for DHCP-assigned addresses. The following list contains software levels required for some Document Centres:

- DC 220/230/332/340 (System software 1.12.62 and higher)
- DC 240/255/260 (System software version 6 and higher)

Additional Information

Xerox Customer Service welcomes feedback on all documentation - send feedback via e-mail to: USA.DSSC.Doc.Feedback@mc.usa.xerox.com.

You can reach Xerox Customer Support at 1-800-821-2797 (USA), TTY 1-800-855-2880 or at <http://www.xerox.com>.

Other Tips about Xerox multifunction devices are available at the following URL: <http://www.xerox.com/DocumentCentreFamily/Tips>.

XEROX®, The Document Company®, the digital X®, and all Xerox product names are trademarks of XEROX CORPORATION. Other trademarks belong to their respective owners.

Copyright © XEROX CORPORATION 2003. All Rights Reserved.

