Chapter 6 - Internet Primer

This chapter is intended to be very basic primer regarding accessing the Internet from your home PC. Some discussion of Internet Access from your OpenVMS System is also included to help fill the gaps in the documentation for software such as UCX and the like.

By the way, the word is "primer" (rhymes with "timer")! That's "pri-" (rhymes with "cry") and "-mer" as in "mermaid". If it was pronounced "primmer", (rhymes with "dimmer"), it would be spelled with two "m"'s in the middle, between the two vowels. Congratulations! You've just had (quite possibly) your first lesson in "phonics".

Back to business. First we'll discuss a little bit about networking, then we'll get into the real meat of the matter. We'll even touch on the mysterious "WINsock" (nothing like a sweat sock, or even a Christmas stocking). Yes, friends, this discussion will center on Windows based software. Whether you're talking about Windows V3.1, Windows for Workgroups (V3.11) or Windows/95, the following discussion is fully applicable. There are some minor differences in Windows/95.

6.1 Internet Access Demystified

The process of accessing the Internet from your home computer is really not much different from dialing into your employer's computer from home, or dialing into the SYS$COMMAND BBS. What **IS** different is what happens once that connection is made.

Briefly stated, you use an application called a "dialer" to establish the link to the Internet. Once that's done, you can use FTP (File Transfer Protocol) or a Web Browser or whatever.

Later on in this chapter, we'll talk more about IP (Internet Protocol) and TCP (Transmission Control Protocol). That portion of this information will deal more with how you might access the Internet at work.

6.1.1 Internet Access Over A Dial-up Line (Modem)

Normally, when you're just dialing up as a terminal user, the data which crosses the dial up link is simple asynchronous serial data. You type a character, it goes to the host, the host (hopefully) "echoes" that character back to your terminal and it

appears on your screen. Of course, passwords should never echo (or you may receive an asterisk ("*") for each character that you type), and when you press a function key like PF1 or something else, the software responds appropriately rather than echoing the escape sequence which that key transmits to the host.

When you dial into an ISP (Interner Service Provider), the data which crosses the link is "framed" in a network data "packet". This framing or packetization comprises a "protocol" like PPP (Point-to-Point Protocol) which allows part of your network link to the Internet to be carried over that dial-up line. Although it's a poor comparison, PPP can be thought of in networking as being what the LAT (Local Area Transport) protocol is to asynchronous serial data links. It's a way to get your data from your workstation (PC) onto the network and vice-versa.

6.1.2 PPP, DHCP and IP

Wow! Hope you're ready for some alphabet soup, 'cause here it comes!

Now that you're "on the net", so to speak, by PPP, what next?

Well, if you're familiar with DECnet, you already know that each "node" on a network needs a unique address. In DECnet, you as the system manager assign the DECnet address (either in cooperation with your network manager, or you may also be the network manager since OpenVMS people tend to wear many, many hats).

So how does your workstation or PC get an IP (Internet Protocol) address?

Well, that's what DHCP is all about. DHCP stands for Dynamic Host Control Protocol. It provides a means by which a server assigned to the task can give you (your workstation or PC), dynamically, an I.P. address from a pool of addresses that have been set aside. No one else in the world has (the right to use) the I.P. addresses in your ISP's (Internet Service Provider's) DHCP address pool.

6.1.3 Internet Access "Dialers"

The "dialer" is really a misnamed little piece of software because while it does serve that purpose, it really does something more - more important that just dialing the phone via the modem.

The dialer is what connects your Windows software to the "network stack", and the network stack to the Internet Service Provider (ISP).

What's a "network stack"? It's a purely figurative term referring to the layers of network software that when properly coordinated allow your computer to connect to other computers (including the Internet) via some kind of network.

The dialer is the first part of the scenario that differs from just dialing into your employer's computer or into a BBS.

To connect your workstation or PC to your Internet Service Provider (ISP), you first use the dialer to dial into the ISP's facility. The dialer's job then is to complete the DHCP negotiations and other portions of establishing the link.

Once the dialer has done it's work and you're connected, then, you can minimize the dialer and open up your Internet application (FTP, Web Browser, etc.).

6.1.4 "WINsock"

So what in creation is "WINsock"? Well, think of it as the link between your Windows operating system and the Network Interface driver. Note that the "network interface" may be an Ethernet or Token-Ring card in your workstation or PC, or it may be one of your COM ports, as is the case when we are talking about dial-up links. It equates (VERY!) roughly to the NETACP process on DECnet Phase-IV systems. The "socket" paradigm comes from the concept of connecting or "plugging in" to a network connection of some sort.

6.2 Internet Protocol (IP) and Transmission Control Protocol (TCP)

To get connected to the Internet, you don't necessarily need to know the information that follows. But since you're probably curious, here's enough to whet your appetite.

Internet Protocol (IP) is the name given to a protocol definition for the protocol used universally on the Internet. IP provides what's known as an "unreliable" connection. That is, there's no guarantee that any IP packets you transmit via the Internet will ever reach their destination, or even traverse the Internet. That's where Transmission Control Protocol (TCP) comes in.

Transmission Control Protocol (TCP) provides a set of defined standards by token of which some guarantee is made that packets transmitted will be acknowledged by the receiving station, or will be retransmitted if a negative acknowledgement is received within a specified time. TCP is really what makes IP a realistic approach to networking. Otherwise, you'd just be be "shouting upwind into a hurricane".

IP addresses look a little like DECnet addresses, except that they have four parts instead of two. For comparison:

DECnet: aa.nnnn

IP: xxx.xxx.xxx.xxx

In DECnet, you have an area number which is separated from the node number by a period (".").

In IP, you have a four-part address than can be broken down into a "network id." and a "node number". This is accomplished by way of what's known as a "subnet mask". The subnet mask tells IP which portion of the address identifies the network and which portion identifies the node.

There is no "easy" way to explain the concept of the subnet mask. That's because it involves converting decimal numbers to binary and vice-versa. All the same, the easiest way to explain the subnet mask goes something like this:

```
Subnet Mask        255  .   255  .     0  .     0
                11111111.11111111.00000000.00000000
```

Notice how there are a group of contiguous "1"'s. Where that group of ones ends is the end of the network identifier. Everything after that is the node identifier.

So, using that as an example:

```
IP Address         192  .    32  .   242  .    17
                11000000.00100000.11110010.00010001

Subnet Mask        255  .   255  .     0  .     0
                11111111.11111111.00000000.00000000
```

With the IP address 192.32.242.17 and a subnet mask of 255.255.0.0, the network identifier is 192.32 and the node number is 242.17. And yes, that is a "Class B" address and subnet mask

Now, there are enough books out there in the bookstores and computer stores to tell you the rest of the story. What we've done here is enough to get you started.

6.2.1 Internet Protocol (IP) on LANs and WANs

In the previous discussion, it may have occured to you that while there are four parts to an IP address, eand each part can have a value as high as 254 (yes, 254! Why? That's beyond the scope of this discussion), this still ends up leaving a dearth

of available addresses. It's still better than DECnet's 63 * 1023 nodes in a global network, of course.

Why is that important? Well, since the subnet mask tells the IP software what part of the address is the network identifier, either you have as many nodes as networks (a class B address), very few networks but many, many nodes (a class A address) or many, many networks and very few nodes (a class C address).

So what IS an IP network? Simply stated, and group of IP addresses where the network identifier is the same. As we discussed earlier, which portion of the IP address constitutes the network identifier is determined by the subnet mask.

6.2.2 Routing and Bridging

In order to communicate across networks, IP routers are needed. The more networks we have, the more routers we are likely to need. Again, "what a router is" is beyond the scope of this discussion. You also need to be able to identifiy a network, which is where the subnet mask comes in (see section 6.2).

There are two kinds or routers. Since they usually perfom the routing and bridging functions simultaneously, we frequently refer to them as "bridge/routers" or "brouters". For this discussion, we'll just focus on routing. The actual difference between bridging and routing is beyond the scope of this discussion.

6.2.2.1 Local Area Network (LAN) Routers

A LAN router has at least two Ethernet or token ring interfaces. If the unit provides protocol conversion, it may have one of each, at least. A LAN router connects two geographically proximate Local Area Networks (LANs) and routes traffic between them. This type of unit would very likely also be bridging some traffic between the networks.

6.2.2.2 Wide Area Network (WAN) Routers

A WAN router has at least one Ethernet or token ring interface and one or more high-speed synchronous serial interfaces of some kind. The high-speed synchronous serial interface is how the router connects its LAN to another, geographically remote network by some kind of link, such as a frame-relay link, an Asynchronous Transfer Mode (ATM) link, an X.25 link, etc. Here again, this unit would very likely also be bridging some traffic between the networks.

6.2.3 Links to the Internet

If your company has a link to the Internet, it will be by some kind of WAN router, perhaps even a specialized type of WAN router known as a "firewall". What's a firewall? Simply stated, it protects your corporate network from unwanted traffic which may try to enter your network from the Internet.

Firewalls are a gallant effort to keep your network secure. It is important to understand, however, that ANYthing can be hacked! ...and if someone tries to tell you otherwise, RUN!!! ...in the opposite direction just as fast as your legs will carry you! (The physically challenged shoudl take last phrase metaphorically, but none the less seriously.)

6.3 Internet Protocol (IP) Summary

In this brief discussion, we tried to cover as much as we could without writing YANM (Yet ANother Networking Manual). Again, you'll find a veritable plethora of books in the bookstores, computer stores, the Internet marketplaces, and many other sources. There's no need for us to go any deeper here.

The author just wanted you to know a little more abou the Internet, since that's where th future will take you, like it or not. You may as well get hip to it, even if your employer is taking a "head in the sand" approach, perhaps complaining that people "get enamoured with their systems" and that seminars and symposia (like the DECUS symposium) held in large cities are just "excuses for expensive, non-productive junkets". (These comments were actually made by former employers of the author.)

For now, though, The SYS$COMMAND BBS will make available to you those OpenVMS resources that you might otherwise miss out on. When your employer asks, "Where did you find that?", just say, "It's from the Internet" and then smile REAL BIG!