Building a WAN PPP link with the EasyServer II using Dial-on-Demand

Keywords: EasyServer II PPP Dial-on-demand DOD routing Windows 95 NT UNIX WAN

Introduction

The purpose of this application note is to provide a solution to the common networking scenario where a remote site needs to be connected to a main site via inexpensive, low-speed dial-up connections, especially where cost minimisation is a factor. The remote site requires full access to the computing resources available at the main site, including remote terminal access, file and printer sharing, electronic mail, and Internet and Intranet access.

This application note will discuss the various issues that arise in providing the connection between the remote office and the main office and how these issues can be solved.

As the access to all of the systems at the main site and to the Internet via the main site is intermittent, it was deemed that a dial-on-demand PPP connection from the remote site would be most appropriate, as opposed to a permanent PPP connection. Dial-on-demand PPP connections are also useful when using dial-up services that are charged on a time basis (e.g. long distance calls).

Scenario Overview

The main network (Network A) consists of a heterogeneous mix of Windows NT and UNIX servers and Windows clients (not shown). The remote network (Network B) consists of Windows 95 clients. The two networks are to be connected using the EasyServer II from Stallion Technologies (two) and a pair of modems (33.6 kbps modems were used).

This Application Note will outline the issues involved in connecting these two networks together and the configuration required in the EasyServer II's that provided the required access for both these networks. The diagram below indicates the networks involved and the IP addresses or address ranges used for the components in the networks.

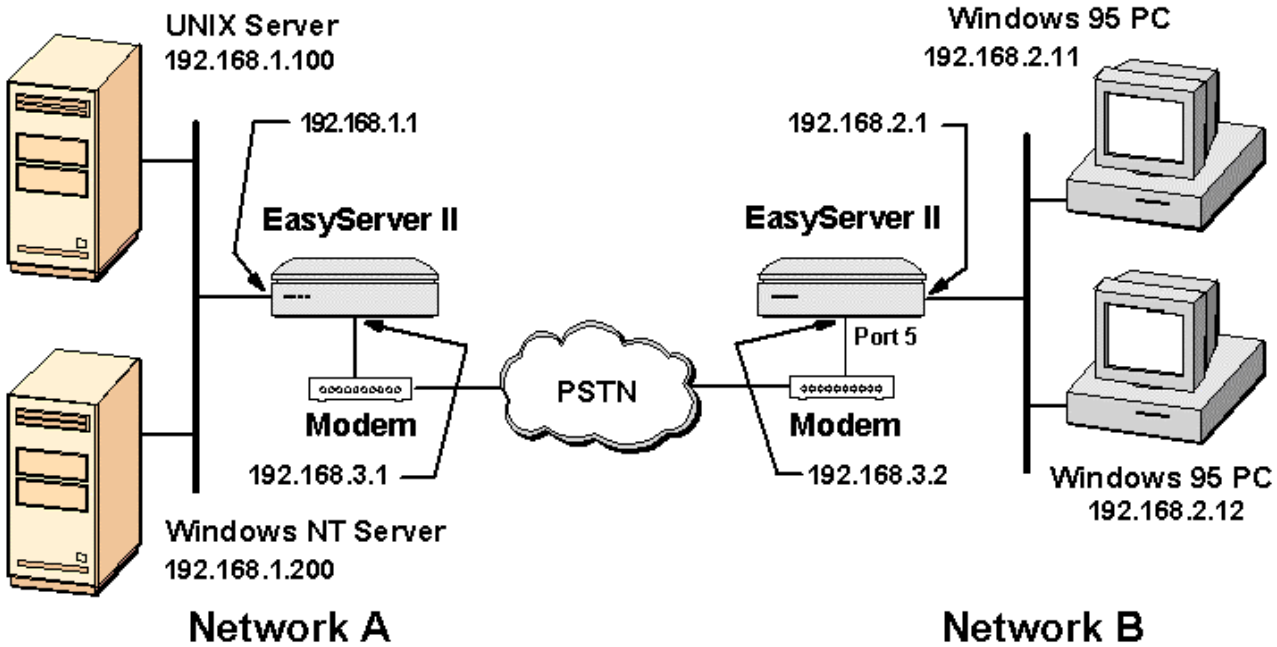

Figure 1 - Network Diagram showing main and remote networks and the PPP link.

Requirements

Apart from the workstations themselves and an Ethernet hub or Thin-net (10Base-2) network to connect them together, all that is required at the remote office is an EasyServer II with the Dial-on-Demand feature enabled and a modem plus an RJ-45 to DB25 modem cable to connect the modem to an EasyServer II port. On the head office network, an EasyServer II, modem and another RJ45 to DB25 modem cable was required.

NOTE:	Before attempting to extend a TCP/IP network, careful consideration should be given to network design, layout, subnet requirements and IP addressing.

This scenario uses IP networks from the 192.168.X.X address space. Three networks have been used, 192.168.1.0 for the main network (Network A), 192.168.2.0 for the remote network (Network B) and 192.168.3.0 for the interconnecting PPP link network. All addresses use a subnet mask of 255.255.255.0.

Hardware Configuration

On the remote network, the two Windows 95 PC's and the EasyServer II are connected together using a simple hub or Thin-net network. This allows the two PCs to access information on each other, such as sharing files and printers. The EasyServer II is connected to the hub or Thin-net and the modem is connected to one of the EasyServer II serial ports.

On the main network, the EasyServer II is connected to the network via the EasyServer II's UTP or BNC ports and the modem is connected to one of the EasyServer II's serial ports.

Both modems need to be connected to an available analogue phone line.

Remote EasyServer II Configuration

The configuration of the remote EasyServer II can be broken down into a number of steps. At certain times, as the EasyServer II is being configured, it is possible to test the configuration to ensure it is correct

Initial Setup

The first thing to do with an unconfigured EasyServer II is to allocate the unit an IP address. This is normally done by connecting a terminal to port 1 of the EasyServer II (with communication parameters set to 9600 bps, 8 characters, 1 stop bit, no parity and software flow control), powering up the EasyServer II, and entering the IP address and subnet mask when prompted (after pressing ¿ **ENTER** a few times). The diagram at right shows the output from an EasyServer II during boot and IP address setup.

After this the unit is ready for configuration. Login to the unit by pressing ENTER several times until a login prompt appears. Press ^Z (CTRL-Z) to get to the command prompt and enter privileged mode by typing:

SET PRIVILEGED ¿ **ENTER**

```
Stallion Technologies, EasyServer ESII-8

Copyright (c) 1996 Stallion Technologies Pty. Ltd., All Rights Reserved.
Copyright (c) 1980, 1986, 1988 Regents of the University of California.


ESII-8   Communications Server V6.0.0  Uptime:     00:00:01

Ethernet:       00-60-1f-00-17-61       Internet:       0.0.0.0
Name:           ESII_00601F001761       Number:         0

Determining IP address from network ...

Requesting BOOTP: No valid response.
Requesting RARP: No valid response.

Server is unable to determine internet address from network.
To manually enter the address, press RETURN key a few times now.
Otherwise server will retry BOOTP and RARP in two minutes.
Server will retry BOOTP and RARP if nothing entered in two minutes.


Enter internet address: 192.168.2.1
Enter internet subnet mask (default is 255.255.255.0):

ESII-8 Communications Server is ready.
```

and typing in the default password "system" when prompted.

Type the command:

SHOW CHANGES ¿ **ENTER**

to view the current active configuration of the unit (stored in the operational database).

Assuming the unit has not been previously configured you should see something similar to the figure at right.

```
ESII-8    Communications Server V6.0.0

Port  1:          PORT_01
Terminal:         ansi  [Status Line]
Username:         None

Enter username: ^Z

Please type HELP for assistance
Local 1> set privileged
Privilege password:
Local 1>> show changes

#
# ESII-8 Configuration changes - extracted from server "ESII_00601F001761"
#
SET INTERNET ADDRESS 192.168.2.1 SUBNET MASK 255.255.255.0
SET PORT 1 TERMINAL ansi
SET PORT 1 USERNAME PORT_01
SET SERVER STARTUPFILE LS-8.CFG HOST None

Local 1>>
```

Basic Port Setup

The port on the EasyServer II is to be configured for a fixed speed of 115200 bps, 8 data bits, no parity, hardware flow control and modem controls. Port access is set to dynamic to allow for possible connections being initiated from the head office network. A section of the configuration required to achieve this is listed below. This assumes we are connecting the modem to port 5 and that the modem is capable of handling a DTE speed of 115200 bps.

NOTE:	The EasyServer II has an operational database and a permanent database for storing unit configuration and operating parameters. The SET command only changes the operational database, the DEFINE command only changes the permanent database, and the CHANGE command modifies both databases simultaneously.

```
CHANGE PORT 5 AUTOBAUD DISABLED
CHANGE PORT 5 MODEM CONTROL ENABLED
CHANGE PORT 5 PPP ENABLED
CHANGE PORT 5 SPEED 115200
CHANGE PORT 5 STOP BITS 1 FLOW CONTROL CTS
CHANGE PORT 5 ACCESS DYNAMIC
```

NOTE:	To perform configuration of the EasyServer II you must either Telnet to the unit or configure the unit by attaching a terminal to port 1 and enter privileged mode. The default privileged mode password is *system*. See the EasyServer II manuals for further details.

Detailed in the diagram above are the IP addresses of the various components of the network. The commands to configure the remote EasyServer II for this location are as follows:

```
CHANGE PORT 5 PPP LOCAL ADDRESS 192.168.3.2 HOST ADDRESS 192.168.3.1
CHANGE PORT 5 PPP SUBNET MASK 255.255.255.0
```

This assumes that the remote EasyServer II has already been allocated the IP address 192.168.2.1 and a subnet mask of 255.255.255.0 during initial configuration. See the EasyServer II manuals for details.

Dialer Setup

A script has to be devised that will cause the modem to dial the appropriate phone number and initiate the PPP connection. This mechanism is called a dialer script. The EasyServer II connected to the main office network

is configured with LOGIN ACCOUNT ENABLED, so a username/password sequence will be encountered during establishment of the PPP connection (see the central network configuration below).

The dialer script, named DOD_DIAL below, sends an "AT" command to the modem, expects a response of "OK" and then dials the number. A 60 second timeout is allowed for the number to be dialed, the remote modem to answer and then the two modems to synchronize. The IP addresses associated with the dialer script are the same as those configured for the PPP connection. The phone number is supplied from elsewhere in the configuration.

When the modem connection is established, the main office EasyServer II will respond with a prompt ending in "name:". After supplying a username, a password will be expected. The prompt will be "word:".

CHANGE DIALER dod_dial PROTOCOL PPP
CHANGE DIALER dod_dial SCRIPT "AT OK ATDT\T TIMEOUT 60 >>
name: <*USERNAME*> word: <*PASSWORD*>"
CHANGE DIALER dod_dial LOCAL ADDRESS 192.168.3.2 HOST ADDRESS 192.168.3.1
CHANGE DIALER dod_dial SUBNET MASK 255.255.255.0

NOTE:
1. The >> designates the command continues onto the next line since there is insufficient space to fit the command on one line. Please do not type these characters yourself.
2. IMPORTANT: there is a space between “name:” and <*USERNAME*> and between “word:” and <*PASSWORD*>.
3. The entire <*USERNAME*> including “<” and “>” should be replaced by a user name. Similarly for <*PASSWORD*>. The quotes in the above commands are required.
4. The dialer script relies on the modem generating verbose responses. The modem should be configured to generate verbose responses when initiating calls only, not when answering calls. The appropriate Hayes AT commands are V1 Q2. These commands may differ among modem manufacturers.

For this exercise we will set the user name to “doduser”.

The dialer script can be tested at this point by using the following command:

CONNECT DIALER dod_dial DIAGNOSTICS ENABLED PHONENO <*phone_number*>

where <phone_number> represents the phone number to be dialed. This will initiate the dialer and modem commands and responses will be shown on the screen. Eventually a message will indicate that a PPP session has been established. The Figure at right shows an example output after running the CONNECT command. You can then test the connection by pinging the remote PPP interface.

If there are any problems encountered at this stage, then they should be resolved before continuing. If the dialer script does not work, then

```
Local 10>> connect dialer dod_dial diagnostics enabled phoneno "0,55512345"
Local -129- Dialing "dod_dial" on port 5
send (AT)
expect (OK)
AT^M^M^JOK
got (OK)
send (ATDT\T)
timeout set to 60 seconds
expect (name:)
^M^JATDT0,55512345^M^M^JRINGING^M^J^M^JCONNECT
26400^M^J^M^J^M^JDetermining term
inal type ... ^[ 0^M^J^M^J^[[2J^[[H^M^JLS-4x4  Communications Server V6.0.0 ^M^
J^MLantra4x4 Dial-in server MR^M^J^M^JPort  5:      3876-7644^M^JTerminal:
ansi  [Status Line]^M^JUsername:
got (name:)
send (dod_dial)
expect (word:)
        None^M^J^M^JEnter username: doduser^M^JAccount password:
got (word:)
send (password)
Local -133- Dialer connection [dod_dial] established
Local -063- Starting PPP datalink session on port 5

Local 10>> ping 192.168.3.1
```

there is no chance that the Dial on Demand connection will work.

Once the dialer has been successfully tested, any active connections should be terminated before using the dial-on-demand facility to initiate a connection. This can be achieved by issuing the command:

LOGOUT PORT X

Where X will be the port associated with the dialer. In this example, port 5.

Filters

Defining the filters is the most important part of configuring a dial-on-demand connection. This is because the filters determine what sort of network traffic initiates the dialer and keeps the connection up. Keeping the connection up unnecessarily increases costs. Not keeping the connection up long enough can adversely affect response time and performance. The commands below setup a filter called DOD_FILTER. The filter is a series of rules that specify which protocol (plus an optional port number) will be accepted/rejected for transmission and whether that protocol will initiate the dialer (determined by the presence of the number, indicating the timeout value, after the ACCEPT or REJECT). Note the number of the entry. The order of the rules is important since the rules get processed in the entry order when determining how a packet should be processed. Thus if you allow all TCP packets to be transmitted in entry 1, stopping some types of TCP packets in a subsequent entry will have no affect.

```
CHANGE INTERNET FILTER dod_filter ENTRY 1 RULE TCP accept 300                          (1)
CHANGE INTERNET FILTER dod_filter ENTRY 2 RULE UDP udp_dport=53 accept 60              (2)
CHANGE INTERNET FILTER dod_filter ENTRY 3 RULE UDP accept                              (3)
CHANGE INTERNET FILTER dod_filter ENTRY 4 RULE ICMP icmp_type=8 accept 60              (4)
CHANGE INTERNET FILTER dod_filter ENTRY 5 RULE ICMP accept                             (5)
```

Notes on line:

1. sets a rule that allows any TCP packet to initiate the dialer with a timeout of 300 seconds. The timeout indicates that the connection will drop after 300 seconds of inactivity.
2. allows UDP packets with a port of 53 (name service or DNS) to initiate the dialer with a timeout of 60 seconds.
3. allows UDP packets to be transmitted whilst the link is active but not to initiate the dialer (due to the lack of a timeout value).
4. allows ICMP (ping) packets with an ICMP type of 8 (ICMP echo-request) to initiate the dialer with a timeout of 60 seconds.
5. allows ICMP (ping) packets to be transmitted whilst the link is active but not to initiate the dialer (due to the lack of a timeout value).

After the initial filter configuration, it was noticed that a connection was being initiated every 12 minutes. At these times, there were no active connections. Investigation revealed that the traffic was due to normal Windows Networking Browser traffic where one of the remote Windows 95 PC's, having been elected the local browse master for that LAN, was trying to contact the master browser of the main LAN to share browse list updates. This network traffic was destined for TCP port number 139. There are two other TCP port numbers associated with Windows networking traffic. These are ports 137 and 138. It is was decided to prevent any TCP traffic destined for these ports to initiate a connection to the main network, but allow the traffic if the connection to the main network was already established. To prevent the dialer from being initiated in this way the following rules were added to the filter:

```
CHANGE INTERNET FILTER dod_filter INSERT 1 RULE TCP tcp_dport=139 accept
CHANGE INTERNET FILTER dod_filter INSERT 1 RULE TCP tcp_dport=138 accept
CHANGE INTERNET FILTER dod_filter INSERT 1 RULE TCP tcp_dport=137 accept
```

These rules need to be inserted before the existing ENTRY 1 since they need to be in the list prior to the rule which accepts all TCP packets and allows them to initiate a dialer. The order of rules is important since the first match in the list of rules will be the one that determines how a packet is processed.

Dial-on-Demand Setup

The final step in the process is to setup dial-on-demand to use the dialer and filter that we previously created and to specify the phone number to dial. This phone number is passed to the dialer as a variable (\T in the dialer script). The following commands configure a dial-on-demand entry called *access* for use:

```
CHANGE INTERNET DOD access DIALER dod_dial
CHANGE INTERNET DOD access FILTER dod_filter
CHANGE INTERNET DOD access PHONENO "0,0912345678"
CHANGE INTERNET DOD access ENABLED
```

Note the quotes around the phone number. This is only necessary if you are using a comma (",") to insert a one second delay between digits in the phone number. This delay is sometimes used when inserting a delay between the number to obtain an external phone line and the number of the line to call. The number used to obtain an external line is only needed when you have a PBX and this number is typically 0 or 9.

Complete Setup

The full remote EasyServer II configuration is as follows:

```
CHANGE INTERNET ADDRESS 192.168.2.1 SUBNET MASK 255.255.255.0
CHANGE INTERNET GATEWAY 192.168.3.1 NETWORK ANY
CHANGE PORT 5 Autobaud DISABLED
CHANGE PORT 5 Modem Control ENABLED
CHANGE PORT 5 PPP ENABLED
CHANGE PORT 5 SPEED 115200
CHANGE PORT 5 STOP BITS 1 FLOW CONTROL CTS
CHANGE PORT 5 PPP LOCAL ADDRESS 192.168.3.2 HOST ADDRESS 192.168.3.1
CHANGE PORT 5 PPP SUBNET MASK 255.255.255.0
CHANGE PORT 5 ACCESS Dynamic
CHANGE DIALER dod_dial PROTOCOL PPP
CHANGE DIALER dod_dial SCRIPT "at OK atdt\T TIMEOUT 60 name: doduser word: <password>"
CHANGE DIALER dod_dial LOCAL ADDRESS 192.168.3.2 HOST ADDRESS 192.168.3.1
CHANGE DIALER dod_dial SUBNET MASK 255.255.255.0
CHANGE INTERNET FILTER dod_filter ENTRY 1 RULE TCP tcp_dport=137 accept
CHANGE INTERNET FILTER dod_filter ENTRY 2 RULE TCP tcp_dport=138 accept
CHANGE INTERNET FILTER dod_filter ENTRY 3 RULE TCP tcp_dport=139 accept
CHANGE INTERNET FILTER dod_filter ENTRY 4 RULE TCP accept 300
CHANGE INTERNET FILTER dod_filter ENTRY 5 RULE UDP udp_dport=53 accept 60
CHANGE INTERNET FILTER dod_filter ENTRY 6 RULE UDP accept
CHANGE INTERNET FILTER dod_filter ENTRY 7 RULE ICMP icmp_type=8 accept 60
CHANGE INTERNET FILTER dod_filter ENTRY 8 RULE ICMP accept
CHANGE INTERNET DOD access DIALER dod_dial
CHANGE INTERNET DOD access FILTER dod_filter
CHANGE INTERNET DOD access PHONENO "0,0912345678"
CHANGE INTERNET DOD access ENABLED
```

Main EasyServer II Configuration

The main or dial-in EasyServer II located in the main or central office has a simpler configuration as it is only required to accept dial-in PPP connections. The port setup is almost exactly the same as in the remote EasyServer II. The central EasyServer II configuration is listed below with port 5 setup for dial-in:

```
CHANGE INTERNET ADDRESS 192.168.1.1 SUBNET MASK 255.255.255.0
CHANGE PORT 5 Autobaud DISABLED
CHANGE PORT 5 Login Account ENABLED
CHANGE PORT 5 Modem Control ENABLED
CHANGE PORT 5 PPP ENABLED
```

```
CHANGE PORT 5 SPEED 115200
CHANGE PORT 5 STOP BITS 1 FLOW CONTROL CTS
CHANGE PORT 5 PPP COMPRESS ENABLED LOCAL ADDRESS 192.168.1.1                    >>
                HOST ADDRESS 192.168.1.41
CHANGE PORT 5 PPP SUBNET MASK 255.255.255.0
CHANGE PORT 5 INITIALIZATION SCRIPT "<Insert an appropriate modem initialization script here>"
CHANGE PORT 5 ACCESS Dynamic
CHANGE ACCOUNT pppuser PASSWORD "<password>"
CHANGE ACCOUNT pppuser PROTOCOL PPP
CHANGE ACCOUNT pppuser COMPRESS ENABLED
CHANGE ACCOUNT doduser PASSWORD "<password>"
CHANGE ACCOUNT doduser PROTOCOL PPP
CHANGE ACCOUNT doduser COMPRESS ENABLED LOCAL ADDRESS 192.168.3.1               >>
                        HOST ADDRESS 192.168.3.2
CHANGE ACCOUNT doduser SUBNET MASK 255.255.255.0
```

NOTES:
1. The central unit has LOGIN ACCOUNT ENABLED on port 5 which means the port will always prompt incoming connection for a username and password.
2. PPP host and local addresses have been configured on this port, demonstrating that the port can also be configured for remote access dial-in by other clients.
3. Two user accounts are shown in the above configuration. The account *doduser* has been configured with local and host IP addresses and is used for the Dial-On-Demand situation. These IP addresses will override the settings on the port. The account *pppuser* is a standard PPP account without any IP address information. This means the account will use the IP address information configured for the port. This account could then be used for dial-in Windows 95 clients configured for server assigned IP addresses, for example.

Routing Considerations

In this scenario it has been assumed that the central network is using a dynamic routing protocol called RIP (Routing Information Protocol) which is supported by the EasyServer II, Windows NT and most implementations of UNIX. Thus when the remote EasyServer II dials-in to the central office, it propagates its routing table to the central EasyServer II and so-on to the RIP-enabled computers and network devices. It is for this reason that no gateway entry is required in the central site's EasyServer II. If you were to rely solely on static routes, the following command would need to be set in the central site's EasyServer II:

```
CHANGE INTERNET GATEWAY 192.168.3.2 NETWORK 192.168.2.0 SUBNET MASK 255.255.255.0
```

In this case, the SUBNET MASK is optional as 255.255.255.0 is the default mask for the network 192.168.2.0, it being a C class network. More routes can be added as required to support packet forwarding to networks beyond those mentioned in this scenario.

Your Windows NT and UNIX computers would also need to have the appropriate static routes added to their routing tables so that they could send packets to the remote network.

Windows Wide Area Networking Considerations

To obtain full Windows style network functionality (including network browsing and network logon) in an IP routed network, Windows machines on the remote network require some further configuration. Specifically, to make network browsing work, the windows client needs to know the name of the master browser on the central network so as to share browsing information. These issues can be resolved by using a WINS (Windows Internet Name Server) to resolve NetBIOS names over TCP/IP. Thus remote Windows 95 clients can initiate a dialup connection, find the master browser and/or PDC (Primary Domain Controller) of a Windows NT domain and thus logon to the network and participate in browsing. At least one of the remote Windows 95 clients will require the "Microsoft File and Printer Sharing" service installed with the "Browse Master" option set to "Automatic" or "Enabled". If you use Windows NT computers on the remote network, then these computers will automatically assume the remote subnet master browser role.

If a WINS server is not available then you may want to use an LMHOSTS file for NetBIOS name resolution. This is a simple text file that operates in a similar way to the UNIX style HOSTS file. It lists IP addresses and their corresponding NetBIOS names and some additional parameters for particular entries. See Microsoft TechNet article Q150800 for full details of network browsing with LMHOSTS in TCP/IP networks.

Below is an example LMHOSTS file which would be placed in the windows directory of a Windows 95 client and called LMHOSTS:

```
192.168.1.200          NT_PDC          #PRE    #DOM:NT_DOMAIN
192.168.1.200          "NT_DOMAIN      \0x1b"  #PRE
```

192.168.1.200 is the IP address of the PDC (NT_PDC) of the central site's Windows NT domain (NT_DOMAIN). The first line tells the client the IP address and NetBIOS name of a computer on the network. The #PRE tells the client computer to pre-load the name into the NetBIOS name cache and the #DOM indicates this entry is an entry for a domain controller for domain NT_DOMAIN. The second entry has a special name in quotes that is made up of the domain name (NT_DOMAIN) and spaces that make up a total of 15 characters plus an hexadecimal character denoted by \0x1b. This last character denotes the name is associated with the Primary Domain Controller for the domain NT_DOMAIN. The two entries together tell the Windows 95 client where to contact the central site's domain master browser (which is always the PDC) and what machine can authenticate user login.

See Microsoft TechNet for further information on implementing wide area networks with Microsoft operating systems.

Conclusion

Using Dial-On-Demand is a cost-effective way of providing wide area access to centralized computing resources for remote offices. The EasyServer II is an inexpensive alternative to many "remote access" servers currently on the market and adds the flexibility to be able to integrate the functions of terminal server and remote access device. With the addition of ISDN terminal adapters, high performance wide area links can be established that serve remote LAN's as well as traditional terminals, printers and other serial devices.

Microsoft Windows network services are fully supported as Microsoft has built all of the enabling technologies (such as WINS) to allow remote clients to access Windows network resources across TCP/IP networks.

Careful consideration needs to be given to the setup of the dial-on-demand application, especially the configuration of filters, since this will determine how effective dial-on-demand is at minimizing the cost of the wide area link and simultaneously provide the level of service required.