Application Note

Creating a WAN with ePipe Using Multiple Direct Dial-up Links

Contents

1 Introduction

There are many ways of connecting two LANs (Local Area Networks) together using the wide variety of technologies available today. In a local telephone call area, by far the least expensive of these methods is by using standard analog dial-up modems to connect one LAN to the other. The disadvantage of doing this is the limited bandwidth that analog modems provide, usually 33.6 kbps (as 56 kbps modems can only achieve this speed in one direction when connecting to ISPs with digital telephone services). The alternative is to use more than one modem to connect the LANs together. The problem with this is that a technology is required to *bond* the modem links together, to effectively provide more bandwidth that is transparent to the users on each LAN.

ePipe uses a technology called E^2B (End to End Bonding) which enables ePipe to bond together multiple links between sites over the Internet using the IPSec (IP Security) protocol to authenticate and encrypt the data. E^2B can also be used point-to-point to create a bonded link between two LANs without the Internet being involved. This achieves the aim of connecting the two sites together using inexpensive analog telephone lines and modems while increasing the available bandwidth between the LANs. This application note will step through the process of designing and configuring a connection between two sites using ePipe with multiple modems using E^2B.

2 The Problem

A customer has come to you and asked you to implement a solution using ePipe to connect two networks together with the object of minimizing on-going telecommunications costs, which is why they chose ePipe. They need up to 100kbps of bandwidth. Their network is completely TCP/IP based.

3 Designing the Solution

When designing any TCP/IP-based communications network, we need to design the network addressing and decide on how the networks will be connected together, that is, what equipment/software is required.

Starting with the IP network design, let us assume the two networks are using the IP addresses in Table 1.

Table 1 - LAN IP Addressing

Network	Network IP Address	Subnet Mask	CIDR Form[†]
Head Office	192.168.1.0	255.255.255.0	192.168.1.0/24
Branch Office	192.168.2.0	255.255.255.0	192.168.2.0/24

We want to connect these two offices together and we need around 100 kbps of bandwidth between the offices. As analog modems connect at a maximum of 33.6 kbps then 3 modems will provide a maximum of 3 x 33.6 = 100.8 kbps. (Note that 56k modems only achieve up to 56k downstream because they dial into a service provider using digital phone services.) You have decided to use an ePipe 2148 at the remote office as it has 4 asynchronous serial ports and an ePipe 2181 at the head office as you believe this will provide more ports for other purposes, such as remote access (dial-in PPP) or Internet Access. The next step is to draw the network and design the IP address schema.

[†] CIDR = Classless Inter-Domain Routing. Addresses take the form of IP_Address/Number_of_subnet_bits. For example, a subnet mask of 255.255.255.0 is 11111111 11111111 11111111 00000000 in binary which is 24 ones followed by 8 zeros. The ones correspond to the network part of the IP address so the network address 192.168.1.0 with subnet mask 255.255.255.0 can be written 192.168.1.0/24.

The design of the IP network is as anyone familiar with designing routed networks would expect, except that the connection between the LANs uses three (3) PPP links, each of which will require IP addresses for the end points of each link. The next available LAN after 192.168.2.0/24 was chosen, the PPP links being allocated consecutive addresses from this address space. Thus we obtain the IP address pairs listed in Table 2 and displayed in Figure 1. These IP addresses are allocated by the ePipe acting as the PPP server.

Figure 1 - Physical Network Design with IP Addressing

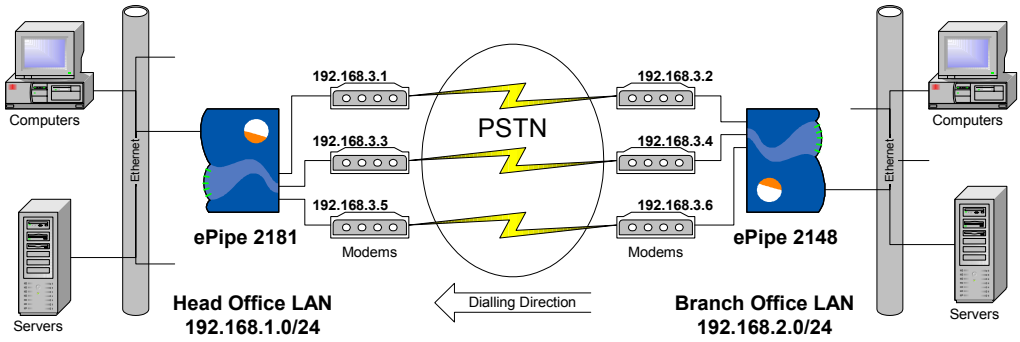


Table 2 - PPP Link IP Addressing

PPP Link on Port Number	Local IP Address	Remote IP address
1	192.168.3.1	192.168.3.2
2	192.168.3.3	192.168.3.4
3	192.168.3.5	192.168.3.6

We also need to assign addresses to the ePipes on the LANs they are connected to. Let us use the first IP address on each LAN for the ePipe, therefore the ePipe 2181 will have an IP address of 192.168.1.1 and the ePipe 2148 will have an IP address of 192.168.2.1.

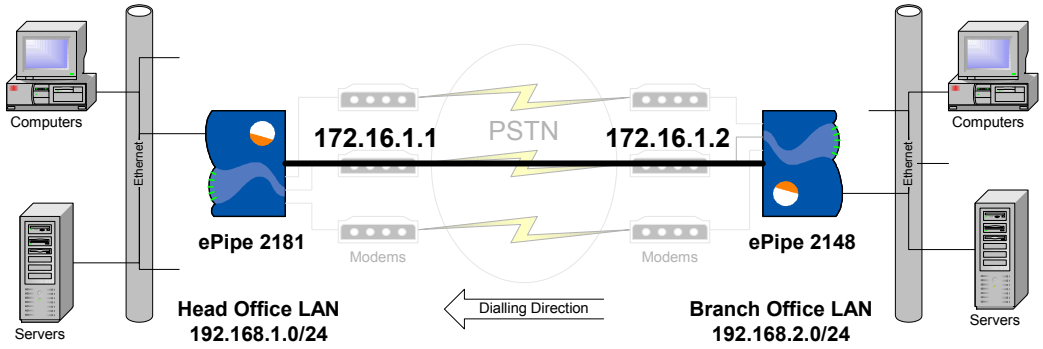
The actual technology bonding these links together is E²B, which establishes an IPSec based tunnel between the ePipes. As this tunnel is a (virtual) point-to-point connection from one LAN to another, for routing reasons it also needs to have IP addresses allocated to the tunnel end points. These addresses are used only within the ePipes' routing tables and can be selected from any address space that is not in use elsewhere in your network. For this design, the private IP addresses listed in Table 3 have been used. Note that the local and remote addresses are from the perspective of the ePipe acting as the tunnel server.

Table 3 - IPSec Tunnel End Points IP Addressing

Local IP Address	Remote IP address
172.16.1.1	172.16.1.2

Figure 2 shows the network design with the virtual (tunnel) connection and its IP addresses. Note how similar this is to designing a traditional point-to-point WAN (Wide Area Network). The physical modem connections have been grayed out. The tunnel is also like a dial-up connection in that the "client" end of the tunnel dials (or connects to) the "server" end of the tunnel. In this case the ePipe 2148 establishes the tunnel to the ePipe 2181.

Figure 2 - Network Diagram Showing Virtual Link and IP Addressing



The last part of the design involves selecting the appropriate ePipe Feature Sets to enable this solution. As an IPSec tunnel (using E²B) is required, the SSV (Site to Site VPN) Feature Set will be required for both ePipes. The ePipe dialing out needs SIA, which is a standard feature of all ePipes. The ePipe receiving the dial-up connections is acting as a PPP server and will need the DCS (Direct Connection Services) Feature Set to enable this option. Feature Set requirements are summarized in Table 4.

Table 4 - Feature Set Requirements

Feature Set	ePipe 2148 (PPP Dial-out & Tunnel Client)	ePipe 2181 (PPP & Tunnel Server)
SIA	Standard	Standard
SSV	Required	Required
DCS	Not required	Required

This essentially completes the design of the network.

4 Implementation

Let us call the ePipe making the dial-out PPP and tunnel connections the *client* and the ePipe receiving the dial-in PPP and IPSec tunnel connections the *server*.

The steps to install a multiple dial-up connection between two networks using E²B are outlined below:

1. Activate the appropriate Feature Sets in each ePipe.
2. Configure the Server ePipe to receive PPP connections.
3. Configure the Server ePipe to receive an IPSec tunnel connection.
4. Configure the Client ePipe to establish PPP connections.
5. Configure the Client ePipe to establish an IPSec tunnel connection.

Each of these steps is covered separately below.

4.1 Activate the appropriate Feature Sets in each ePipe

The easiest way to obtain Feature Set Activation Keys is by following the instructions on the Feature Set Registration Card, which you will have received when you purchased the Feature Set. Alternatively, use a web browser to browse to the Setup page of the ePipe Management Assistant and click on the icon to the left of the Feature Set name and follow the instructions.

The ePipe Management Assistant refers to the inbuilt web server of the ePipe, which provides setup wizards, status information and help, allowing easy

configuration of the ePipe. Simply use your favorite web browser (that supports java script) and enter the IP address of the ePipe in the address or URL field.

NOTES

1. Each Feature Set Activation Key is generated from the MAC address of a specific ePipe unit and will not work on any other ePipe.

2. After you "activate" the Feature Set, the ePipe will restart. After 30 seconds you will be returned to the ePipe Setup page. The status of the feature sets should now reflect the addition of a new feature (or features). If not then repeat the process of activating the feature, as the most likely cause is a mistake during key entry. Also ensure that the key supplied is for the ePipe with the correct MAC address.

4.2 Configure the Server ePipe to Receive PPP Connections

The DCS (Direct Connection Services) Feature Set enables the ePipe as a PPP dial-in server, which enables other computers with PPP dial-out clients to connect to the ePipe and, hence, to the LAN the ePipe is connected to. This is commonly referred to as Dial-in Remote Access or Dial-Up-Networking (in Microsoft Windows). PPP is the Point-to-Point Protocol and is used in many Wide Area Networks (WANs) to establish dial-up links between networks.

To configure the ePipe 2181 to receive dial-in PPP connections we use the DCS Setup Wizard to setup each port, using the following procedure:

1. Configure the ePipe ports for dial-in PPP connections:

   - Use a web browser to browse to the ePipe 2181 and click on *Setup*.
   - Select the DCS *Setup Wizard* followed by *Incoming PPP Connections*.
   - We will use the default values for authentication methods and compression as these use CHAP (which is more secure than PAP) and compression is enabled.
   - Select the port to configured for dial-in.
   - Insert an appropriate modem initialization string in the box provided. A reasonable default would be:

     ```
     at&c1&d2s0=2 OK-at&c1&d2s0=2\p-OK
     ```

     [This sends the string once and, if a reply of "OK" is not received, sends it again. This fixes problems with modems that may have received bad characters during serial port initialization.]
   - In the local and remote IP address boxes, insert the appropriate IP addresses as listed in table 2. Set the subnet mask to 255.255.255.255.
   - When you are finished, click on *Configure*.
   - You will now be asked for the asynchronous serial port settings. Change these to suite your modem. The default values are usually fine. Click on *Configure* when done.
   - You will now see a message saying you have completed this configuration wizard. Click on *OK* when ready. This completes the setup of this port.

- Repeat the above procedure for all ports receiving PPP dial-in connections. Remember that each port uses different IP addresses.

2. Once all ports have been configured, one or more user accounts will need to be created for the authentication of the PPP connection using the PAP or CHAP authentication protocols. Follow these steps to create user accounts:

   - Use a web browser to browse to the ePipe 2181 and click on *Setup*.
   - Select the DCS *Setup Wizard* followed by *ePipe User Accounts (secrets)*.
   - Select *Create New User Account* then click *Next*. If there are no previous accounts, the ePipe Management Assistant will go straight to *Create a New Account*.
   - Type in a user name and password (twice to confirm) for this user account. A client dialing in will need to provide this username and password to authenticate the connection. Click on *Configure* when done.
   - You can use this single account for all ports or you can create an account for each port. If you choose the latter option, simply repeat this procedure for each account.
   - When you are finished creating user accounts, select *Enough user accounts exist* and click on *Next*.
   - You will now see a message saying you have completed this configuration wizard. Click on *OK* when ready. This completes the creation of accounts.

3. This completes the PPP dial-in configuration.

NOTE	Analog modems and ISDN TAs (Terminal Adapters) can be used on the ePipe asynchronous ports. While analog modems all use a similar command set (based on the AT command set), ISDN modems or TAs have some basic commands in common but differ substantially in other commands. When selecting an initialization script for any modem it is best to read the modem's documentation to see which commands the modem supports.

4.3 Configure the Server ePipe to receive an IPSec tunnel connection.

The bonding of the multiple links is done via an E²B enabled VPN tunnel. This tunnel has a server end and a client end. We are going to setup the server end on the ePipe receiving the PPP connections which should be the 2181. To do this, follow these steps:

1. Using a web browser, browse to the ePipe and go to *Setup*.
2. Click on the *SSV Setup Wizard*, then *Site to Site VPN (IPSec with E2B)*.
3. Click on *Create a new Internet Connection Bundle* then *Next*.
4. Give the bundle a name in the box provide, then click *Next*.
5. Click on *Select the existing Links to use* and then click on *Ethernet 1*. Click *Next* when ready. We create a bundle on Ethernet 1 as we need to use the IP address of the Ethernet port for receiving the tunnel connection from the other ePipe.
6. Select *Don't use a traffic filter* then *Next*.

7. Select *Don't use an IP NAT Rule Set* then *Next*.

8. On the *Configure the Connection Bundle* screen, click *Next*.

9. Now you can start to configure the tunnel. Select *Server Side* and then *Next*.

10. Name the tunnel, the fixed IP will be 192.168.1.1, the local address should be 172.16.1.1 and the remote address should be 172.16.1.2. Click *Next* when finished.

11. Insert the address of the remote LAN. This should be 192.168.2.0 with subnet mask 255.255.255.0. Click *Next* when finished.

12. Insert a local SPI of 1 and a remote SPI of 2. Change the Encryption algorithm and Authentication algorithm both to None. Leave all the keys blank. Click *Configure* when done.

13. Lastly, click "Start VPN Now". This finishes the server end of the tunnel.

NOTE	As the links are connecting directly using direct-dial PPP links, authentication and encryption algorithms have been set to none so as to reduce overhead and increase performance of the tunnel connection. If extra security is required, the authentication and encryption algorithms may be set appropriately, especially if there is a concern over the privacy of information traveling through the PSTN (Public Switched Telephone Network).

4.4 Configure the Client ePipe to establish PPP connections.

Configuring the client ePipe to connect multiple dial-out PPP links to the server-side ePipe is achieved the same way as configuring shared Internet access (SIA). This can be done via the SIA setup wizard on the ePipe setup page. Simply follow the prompts to create a bundle (a group of links to be bonded together) and then create each link and add each link to that bundle. When asked about filters, do not create a filter. Similarly for NAT Rule Sets, do not use or create any NAT rules. Both filters and NAT rules are only useful when connecting a bundle of links to the Internet.

When creating the links, please take note of the following:

- The phone numbers dialed by each link must match the dial-in numbers of the lines configured in section 4.2.
- The user name and password used for each link must match the users created in section 4.2.
- Use dynamic IP address assignment so that the addresses defined in section 4.2 will be allocated to each link during PPP negotiation.
- Turn off or deselect "Use IP NAT" on the modem configuration screen.
- Ensure you select the appropriate modem type from the list provided. If your modem is not listed then select one of the generic modem types. Also ensure you select the correct port for that modem.
- The serial port settings screen allows you to change the communication settings the ePipe uses to talk to the modem. These settings are usually correct for most 56k modems.
- If you want a link to always stay connected or dialed-up, click on the "Bandwidth" button (in blue text, next to the link heading in the Connection

Bundle Manager screen) and change the dialer state to "Static". As the dial-up links are likely to be in a non-time-charged local call zone, it is likely that you will want the links to be connected all of the time.

When you are finished creating links you can test the links by enabling the bundle. To do this, go to the Summary page (in Advanced) and turn the bundle off and then on by clicking on the on/off button next to the bundle name. You can monitor this via the Status > Raw Stats > Bundles page. Other useful things to look at are available from the ePipe command line interface (CLI). Login to the ePipe via the console port or a telnet session and run the command:

MONITOR PORT 1-3 PPP

This will display the status of the PPP connections and includes IP address allocated to the links.

At this point you should have 3 dial-up connections working, however this does not enable them to be bonded together. To do this we must create a client end VPN tunnel to connect to the server end VPN tunnel we created in section 4.3. This tunnel will use the bundle we just created and bond these links together to form a single "pipe" between the two networks.

4.5 Configure the Client ePipe to establish an IPSec tunnel connection

This process is similar to section 4.3 where we made the server end of the VPN tunnel. The client end of a SSV tunnel is the end that establishes the bonded tunnel connection. The server end of a SSV tunnel listens for this connection. To configure the client ePipe to make this tunnel follow the steps below:

1. Browse to the client ePipe and select Setup.
2. Click on the SSV Setup Wizard, then "Site to Site VPN (IPSec with E2B)".
3. Click on "Use an existing Internet Connection Bundle" and select the bundle you created in section 4.4. Click *Next* when ready.
4. Now you can start to configure the tunnel. Select "Client Side" and then Next.
5. Name the tunnel "Direct" (must match the name in section 4.3) and the fixed IP will be 192.168.1.1 (the LAN side IP address of the server ePipe). Leave everything else at the default values. Click *Next* when ready.
6. Insert the address of the remote LAN in the gateway table. This should be 192.168.1.0 with subnet mask 255.255.255.0. This tells the ePipe about the LAN that is reachable across the tunnel. Click *Next* when ready.
7. Insert a local SPI of 2 and a remote SPI of 1 (note these are the reverse of those used on the server end). Change the Encryption algorithm and Authentication algorithm both to None (to match the server end). Leave all the keys blank. Click *Configure* when done.
8. Lastly, click "Start VPN Now". This finishes the client end of the tunnel.

You can monitor this by going to Status > Raw Stats > Bundles and looking for the bundle named after the VPN Tunnel. If it shows CONNECTED then the tunnel is connected. Note that the tunnel cannot connect until at least one of the links in the bundle of links is up. This screen also shows this connection bundle and all of its links.

On the server end you can monitor the VPN tunnel connection by going to Status > Raw Stats > SSV. "CLOSED" indicates no connection while "OPENED" indicates the connection is up.

That completes the configuration process.

5 Conclusion

ePipe's E²B technology is a useful alternative to using multi-link PPP (ML-PPP or MPPP) in cases where two networks need to be connected together to form a LAN and cost is a major inhibitor. Using local calls in regions with un-timed local call zones allows inexpensive links between networks using multiple dial-up connections to be created. This provides more bandwidth at less cost for IP-based data communications between sites that are geographically close to each other.

ePipe provides a flexible solution with the ability to simultaneously connect LANs to the Internet, to each other directly (using Direct Connection Services - DCS) or using virtual private networks across the Internet (with Site to Site VPN - SSV), to remote PCs using Secure Remote Access (SRA) and other devices using terminal services (part of DCS). ePipe can provide an all in one solution and gives you a choice between dial-up and broadband connections.

For more information about ePipe or other ePipe products please see our web site (http://www.ml-ip.com/).

Document Number: AN-EP-001
Keywords: ePipe WAN bonding DCS E²B direct connection

First Revision: Jan, 2001
This revision: September, 2002