Application Note

Connecting to Telstra BigPond Cable using ePipe

1 Introduction

The Telstra BigPond Cable service is offered by Telstra BigPond as part of their Broadband product range for connecting to the Internet. Telstra is an Australian telecommunications company and BigPond is the name of their Internet division (ISP). Telstra BigPond Cable is a Cable Internet service which may be connected to all 2200 series ePipes and all ePipe ServerWare models. More information on this service can be found at the following URL:

http://www.bigpond.com/broadband/cable/products.asp

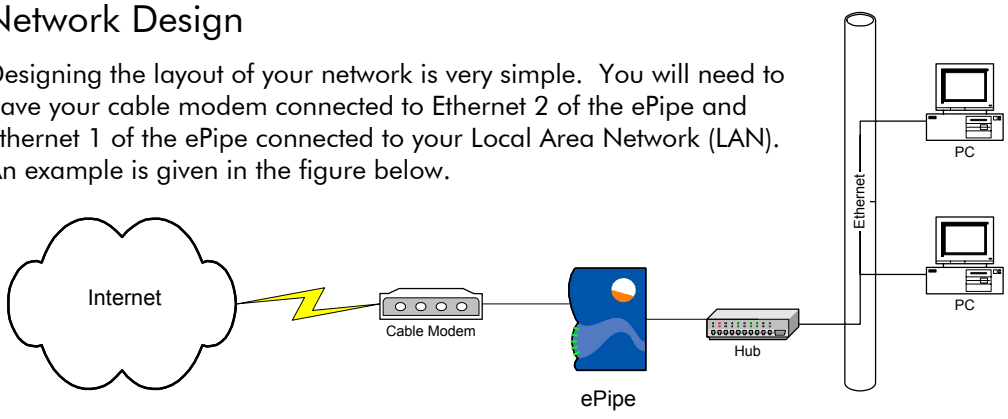
ePipe allows you to connect a network or LAN to the Internet using BigPond Cable. ePipe may act as your firewall, protecting your computer or network from unwanted intruders. At the same time, the ePipe gives you the capability to connect to remote networks using the Virtual Private Network features of ePipe (Site to Site VPN or SSV).

Telstra BigPond Cable uses an authentication mechanism which is based on that of the Road Runner Cable Internet service used by several providers (ISPs) in the US. This system of using client software to identify the user to the Cable service has become commonly referred to as the "Road Runner" system and the clients are referred to as Road Runner clients.

This application note will detail the steps required to connect an ePipe to Telstra Cable using client software based on the Road Runner system of user authentication. Details such as why third party software is required to be used and how to obtain it, how to setup your network, how to configure the ePipe and which filter and NAT rule sets need to be configured within the ePipe are included.

2 Network Design

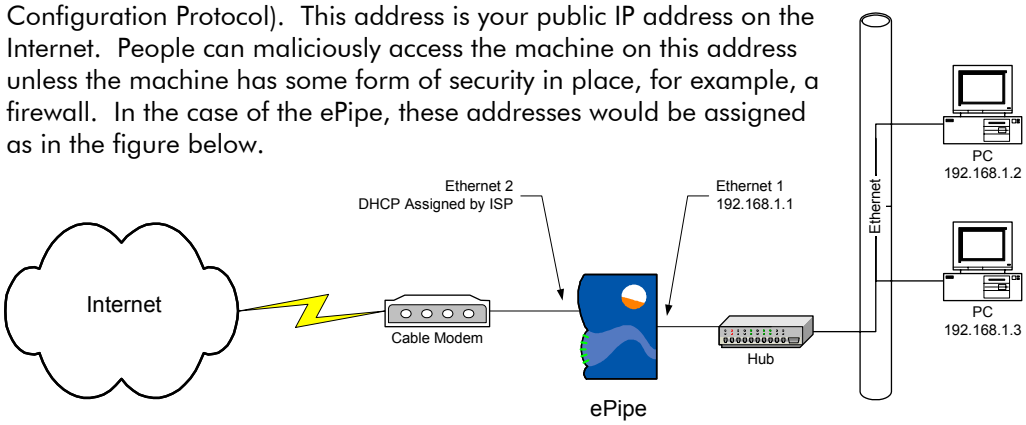
Designing the layout of your network is very simple. You will need to have your cable modem connected to Ethernet 2 of the ePipe and Ethernet 1 of the ePipe connected to your Local Area Network (LAN). An example is given in the figure below.



Each computer on your LAN will need an IP address. The range of IP addresses to be used for your internal LAN should be selected from the reserved or private IP address ranges. Let's use the network IP address 192.168.1.0 with subnet mask 255.255.255.0 for this example. Having setup the ePipe with an IP address of 192.168.1.1 and subnet mask of 255.255.255.0 the PC's on the LAN behind the ePipe will need to be configured with an IP address from this network. In this example, the PCs will have addresses 192.168.1.2 and 192.168.1.3 both with subnet masks of 255.255.255.0. For more information on network addressing, please read the TCP/IP Primer on the ePipe website.

3 BigPond Cable

BigPond Cable uses specific BigPond cable authentication servers to authenticate users and to log users on to the cable network. These servers are region or state specific, with each user having to log on to a server based on the state in which their account lies. Once logged on to the network, the user can access the Internet. Prior to login, Telstra BigPond issues an IP address to the user's PC or ePipe via DHCP (Dynamic Host Configuration Protocol). This address is your public IP address on the Internet. People can maliciously access the machine on this address unless the machine has some form of security in place, for example, a firewall. In the case of the ePipe, these addresses would be assigned as in the figure below.



3.1 How BigPond Cable Works

Telstra uses a heartbeat or Road Runner system to monitor your connection. The BigPond server sends a heartbeat packet to each Road Runner client (usually running on your PC connected to the Cable modem) periodically to determine whether the user is online. A reply must be sent by the client otherwise BigPond Cable assumes the connection has been terminated. Telstra supplies Cable customers with a Road Runner client which will not allow the user to configure the UDP port number to which the BigPond server sends the heartbeat packet during link checking. Thus, when an ePipe is situated between the PC running BPA login and the cable modem, the ePipe cannot forward these heartbeat packets to the internal PC running the road runner client as the ePipe does not know what UDP port the packets will be sent to. Therefore, an alternative client needs to be used which allows this UDP port to be set and known so the ePipe can be configured correctly. A Third party client called BPALogin is available which solves this problem and is available from:

http://bpalogin.sourceforge.net/index.html

3.2 How to install BPALogin

Download version 2.0.1 (or higher) of BPALogin, and then install it on the PC that is going to authenticate the connection. Note that this PC must be turned on and running the BPALogin software for the Cable Internet connection to remain active. Turning the BPALogin client or the PC running it off will eventually cause the Internet connection to stop working.

Install the BPALogin client software, following the installation wizard, until you reach the point where the wizard asks for the type of system you would like to install. The options are:

- Standard Program
  Select this option when installing on Windows 95, 98 or Me or if you wish to manually start the software under Windows NT or 2000.
- NT/2000 Service
  Select this option if you are installing on Windows NT or 2000 and wish the software to be installed as a service.

3.2.1 Using BPALogin on a Windows 9x or ME platform

To install the BPALogin client on Windows 9x and ME platforms, follow the steps below:

1. Complete the installation wizard by clicking *Next*, then *Finish*.
2. To start the program, click *Start*, *Programs*, *BPALogin*, then *BPALogin*.
3. Upon starting this for the first time, a configuration screen should appear.
4. Enter your username and password details and set the port number to be used by BPALogin (the default of 5050 is a good one). This port number will be referred to as the BPALogin port throughout the rest of this document.
5. Enter your BPALogin default domain name. This will be the abbreviation of the state your authentication server is in (either QLD, NSW or VIC) followed by ".bigpond.net.au". For example:

   qld.bigpond.net.au
6. Click OK when done. You will now be able to use the BPALogin client to authenticate with the BigPond Cable server. But firstly the ePipe needs to be configured (see below).

3.2.2 Installing BPALogin on a Windows NT or 2000 platform

To install the BPALogin client on Windows NT and 2000 platforms, follow these instructions:

1. Enter the Username and password details for the cable connection in the spaces provided.
2. Enter the port number the authentication is going to occur on (usually set to port 5050).
3. Select the State you are situated (or authenticating) in.
4. Complete the installation wizard by clicking *Next* twice, then agreeing to reboot your computer when prompted.
5. This completes the setup of BPALogin. Proceed to configuring the ePipe (below).

4 ePipe Configuration

To configure the ePipe for use with the BPALogin client and Telstra BigPond Cable, follow the steps below:

1. Configuring the BigPond Cable Link

(a) Browse to the ePipe and start the SIA Setup Wizard on the Setup page

(b) Follow the wizard through, creating a Bundle and an IPoE link within that bundle. When configuring the IPoE link, note the following:

i. The username field should be left blank.

ii. The IP address is allocated dynamically by DHCP so select "automatic".

2. Setting up Filter Rules

(a) After configuring the IPoE link, filters will need to be configured. Configure the filters for your normal needs (HTTP, HTTPS, FTP, DNS, SMTP or POP3 and E2B (port 2000) if you have a VPN etc) then add some advanced rules for:

i. TCP port 5050 (or the BPALogin port, as specified during installation of the BPALogin client) to allow the authentication request into and out of the network

ii. TCP port 1081 and 8443 out of the network for access to BigPond's online account usage and user management services

3. Setting up NAT Rules

(a) Create a NAT rule set which redirects the BPALogin port (e.g. TCP port 5050) to the IP address of the PC which is performing the authentication. This will allow the BigPond Cable server's heartbeat packets to reach the BPALogin client. This will need to be done using the Command Line Interface, as follows:

i. Telnet to the IP address of the ePipe.

ii. Login as the root user

iii. Create a NAT rule to redirect the heartbeat packets to the PC running the BPALogin client using the following command:

```
CHANGE INTERNET NAT "nat_rule_name" ENTRY n RULE >>
"rdr %s 0.0.0.0/0 port port_num -> ip_address port >>
port_num tcp"
```

Where:

- nat_rule_name is the name of a new or existing NAT rule set (e.g. "Cable NAT Rules").
- ENTRY n specifies the rule number in the NAT rule set. If this is a new NAT rule set then n = 1. If the NAT rule set already exists then n should be one greater than the last rule in the rule set.
- y is the BPALogin port number (e.g. 5050).
- ip_address is the IP address of the computer on the LAN which is running the BPALogin software
- >> indicates the command is broken across two lines for readability.

Example:

```
CHANGE INTERNET NAT "Cable NAT Rules" ENTRY 1 RULE >>
"rdr %s 0.0.0.0/0 port 5050 -> 192.168.1.2 port 5050 tcp"
```

(b) Associate the NAT rule set with the bundle.

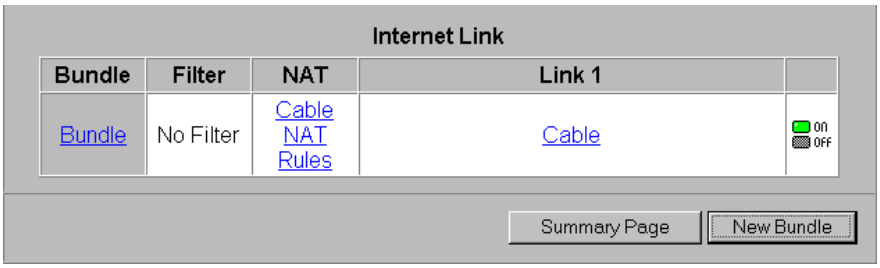
i. If a new NAT Rule Set was created then this rule set will need to be associated with the bundle using these steps:

- Using the ePipe Management Assistant, browse to *Advanced* > *Bundle*.
- Click on the bundle name which has the BigPond Cable link.
- Change the NAT column to the new NAT rule set.
- Click *Configure* when done.

- Turn the bundle OFF and then ON, using the *Advanced* > *Summary* page.

ii. If a NAT rule set already existed and the NAT rule was added to this existing rule set, then the NAT rule set is most likely already associated with a bundle. Use the ePipe Management Assistant to confirm the bundle's current NAT rule set by browsing to Advanced > Bundle. The figure below shows an example.

- If the NAT column for the bundle containing the IPoE link is correct then nothing more needs to be done. If it is not correct, then use the procedure in step 3(b)i above to change the NAT rule set to the correct value.



This completes the setup of the ePipe for access to the BigPond Cable service. To ensure everything is correctly configured, please reboot the ePipe.

5 Other Configuration Issues

To obtain full Internet access, some other items may need to be configured. Consider the following things which may need to be completed to achieve full Internet access:

- The ePipe should be informed of the IP addresses of the ISP's DNS servers by DHCP. If not, you may need to manually configure the ePipe with the IP addresses of the ISP's DNS servers.
- Each PC on the internal LAN should have its default gateway and DNS server set to the internal address of the ePipe (192.168.1.1 in our example).

6 Testing Connectivity

Once the ePipe has been allocated an IP address from the ISP and the BPALogin client has authenticated with the BigPond authentication server, users should be able to access the Internet. The ePipe Management Assistant can be used to check the bundle and link status bye browsing to *Status* > *Raw Stats* > *Bundles*. A status of CONNECTED indicates that the ePipe has been assigned an IP address by DHCP. It does not mean that the BPALogin client has authenticated with the BigPond server or that you can access the Internet. The only way to verify this is to actually browse the Internet, resolve names of computers on the Internet or use a tool such as ping to confirm connectivity.

To confirm Internet connectivity, follow these steps:

1. Access the ePipe CLI (Command Line Interface) via the console port or using a telnet session. Login using the root user.
2. Use the ping command to test connectivity. If name resolution is working properly you should be able to ping the Telstra authentication server using the following command at the ePipe CLI (if ping has been allowed out of the network in the filter rules):

   ping dce-server (sm-server for QLD users)

3. If name resolution is not working then you will need to ping an IP address on the Internet. If you do not know the IP address of a device on the Internet that replies to ping (ICMP echo) then you may need to use a computer that is Internet connected to determine an IP address. Simply use the same ping command as above and observe the IP address of dce-server (sm-server for QLD users). Ping that address directly from the ePipe CLI. Ensure that the PC you are using has the ePipe's IP address as its default gateway and DNS server. Check that the ePipe has had name servers assigned to it using the command:

   SHOW INTERNET NAME RESOLUTION

   If no name servers are listed, you will need to add name servers which should be supplied by the ISP.

To confirm that the ePipe has been assigned an IP address by DHCP, login to the ePipe CLI and run the following command:

SHOW ETHERNET

This will display information similar to the following:

```
Port Ethernet Addr       Internet Addr   Subnet Mask     Flags
-------------------------------------------------------------
1    00-60-1f-00-67-de   192.168.1.1     255.255.255.0   None
2    00-60-1f-00-67-df   0.0.0.0         0.0.0.0         None
```

In this example, Ethernet 2 (port 2 in the output above) shows that an IP address has not been assigned by DHCP. If an address has been assigned it will be listed with its subnet mask and the Flags column will show "Dynamic". No Ethernet 2 address indicates that an IP address hasn't been assigned to you by the ISP. Check connectivity and the link light on Ethernet 2.

7 Conclusion

Using the third party login client, ePipe may be used with Telstra BigPond Cable Internet or other Cable Internet services which use a Road Runner system of authentication. The ePipe provides a firewall for your network to prevent unauthorized access through your 'always on' Internet connection while allowing the Cable service 'heartbeat' to verify your connectivity. With the optional SSV feature key, this ePipe is capable of establishing network to network IPSec VPNs.

Document Number: AN-EP-003
Keywords: LAN Internet Cable Telstra BigPond Firewall

First Edition: August, 2001
This revision: September, 2002