Configuring Demand Routing in AOS

Introduction

The introduction of Demand Routing allows for the creation and termination of dialup links based on more specific parameters than the status of an interface. This guide will provide instructions on using access-lists and tracks to determine when to initiate a dialup connection to a remote location. Further, this guide will also show how to use demand routing for dial-backup.

Hardware/Software Requirements

Demand Routing requires that the following criteria to be met:
- Hardware must be 1000, 3000, 4000 or 7100 series router
- Device needs to run AOS 11.1 or higher
- Unless device is 3120 or 3130, hardware needed includes an Analog or an ISDN BRI DIM daughter board as well as a Netvanta NIM card.

Network Diagram

Example Settings

The following information will be used as example settings for this guide. You should not copy these settings verbatim. You should evaluate this example guide and apply your own settings as needed. Excluding IP addresses, these example settings will always work when connecting two Adtran OS devices.

| Setting	Router A*	Router B
Ethernet IP Address	10.10.10.1	10.10.20.1
Ethernet Subnet Mask	255.255.255.0	255.255.255.0
Demand IP Address	172.16.0.1	172.16.0.2
Demand Subnet Mask	255.255.255.252	255.255.255.252
Local Phone Number	1234567	9876543
PPP Authentication	Sending	Authenticating
PPP Username	TEST	TEST
PPP Password	TEST123	TEST123

*Only steps for Router A are shown in this guide.

Web Interface Configuration

Creating List for Interesting Traffic
Whenever using Demand Interfaces, it is necessary to have a trigger that causes the router to request a pool member to attempt to dial across. In AOS, access-lists are used to allow matching of interesting traffic. To create an Access-List in AOS, first navigate to Firewall/ACLS under the Firewall section on the left side of the screen. The menu options should be similar to below:

After navigating to this page, scroll to the bottom so it displays the Access Control Lists. Click **Configure ACLS** to create ACL to match interesting traffic.
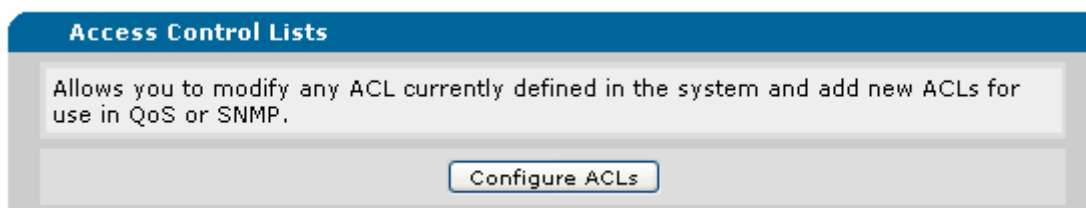
On the next page, type the name of the ACL under ACL name and use extended for the ACL Type. Click Add New ACL.

Access Control Lists

New ACLs can be added by clicking the "Add New ACL" button. Existing ACLs can be modified, deleted, or their evaluation order may be changed using the list below.
WARNING: Removing or modifying an existing ACL could affect network traffic.

Add New ACL

| ACL Name: | Backup | The name to uniquely identify this ACL. |
| ACL Type: | ⦿ Extended
◯ Standard | A standard ACL controls traffic only by the source IP address. |

[Reset] [Add New ACL]

Modify/Delete ACLs

To view or modify an existing ACL, click the "Name" link in the desired row.

| ☐ | ACL Name | ACL Type | Security Zone(s) |

[Remove Selected ACLs]

Click Add New Traffic Selector on the next page.

On Add New Custom Policy Entry, change the Any under Source Host/Network to IP Address and select 10.10.10.0 as the Network and 255.255.255.0 as the Mask.

Source Data

Source Host/Network:
◯ Any
⦿ IP Address
Address: 10 . 10 . 10 . 0
Mask: 255 . 255 . 255 . 0
◯ Hostname

Source IP Address or a hostname of sessions originating in Security Zone 'VPN' that should be affected.

Then, under Destination Host/Network, change from Any to IP Address and use 10.10.20.0 as the Network and 255.255.255.0 as the Mask.

Destination Data

Destination Host/Network:
◯ Any
⦿ IP Address
Address: 10 . 10 . 20 . 0
Mask: 255 . 255 . 255 . 0
◯ Hostname

Destination IP Address of sessions originating in Security Zone 'VPN' that should be affected.

Click Apply to Add the Selector.

Creating a Demand Interface
Click on Demand Routing under Router/Bridge.

Router / Bridge
Default Gateway
Routing
Route table
IP Interfaces
Loopback Interfaces
GRE Tunnels
QoS Wizard
QoS Maps
Bridging
UDP Relay
Demand Routing
VRRP

Insert a 1 into the Demand Number under
Add/Delete/Modify Demand Interface and click Add
New Interface.

Add / Delete / Modify Demand Interface

Add New Demand Interface

Demand Number: 1   Enter demand number (1-1024).

Add New Interface

To view or modify an existing interface and to view statistics for the interface, click the
link in the desired row.

	Number	Description	Resource Pool	State
	There are no configured demand interfaces.			

Remove Selected Interfaces

Under 'Demand 1' Configuration, click the box by enable to activate the
demand interface. Also, name the resource pool (i.e. Backup in this
instance).

'Demand 1' Configuration

Enter the appropriate information below to add demand interface.

Field	Value	Description
Demand Number:	1	Demand interface number.
Description:	Demand 1	Description label (optional)
Enable:	☑	Enable this interface.
Resource Pool:	Backup	Resource pool associated with this interface
MTU:	1500	Maximum Transmission Unit (64-1520)
Fair Queue	64	Subqueue threshold in packets (16-512)
Hold Queue	428	Overall queue limit in packets (16-1000)

Set the connect mode to originate and answer so that either side can establish or respond to a call.

Set the connect mode to originate and answer so that either side can establish or respond to a call.

Select 5 for the Connect Sequence Attempts so it doesn't continually try to dial out.

All the other settings should be left to default. These are more advanced settings than should be needed for a typical demand interface. Under Match Interesting Traffic, select the ACL that was created earlier in the guide. In this case, the ACL was named Backup.

Under Match Traffic Direct, leave this the default of both. This will allow both sides to initiate and respond to a call.

PPP Configuration

In this example, CHAP Authentication will be used to authenticate one side to the other for this call. Since this is Router A, this router will be sending authentication to Router B.

Select CHAP from Sent Authentication Type.

Next, set the Sent Username and Password shown above under the Network Diagram table. "TEST" will be the username and "TEST123" will be the password.

Note: If this would have been Router B, the Sent Authentication Type would have been left as None and the Peer Authentication Type would have been set to CHAP. This would have also resulted in the Sent Username and Sent Password being blank. The username and password would have instead been set under Peer Username and Peer Password.

PPP Configuration

Sent Authentication Type: None

Sent Username:

Sent Password:

Peer AuthenticationType: CHAP

Peer Username: TEST

Peer Password: TEST123

As has been stated, many of the settings for Demand Routing are advanced and unnecessary for a basic configuration; therefore there is really no reason to set PPP Multilink, Interleaving, Fragmentation or the Maximum Number of Multilink interfaces.

IP Settings

For IP connectivity, the IP address of the Demand Interface for Router A needs to be set to the IP address shown in the Network Diagram for that interface (172.16.0.1 Mask 255.255.255.252). Set the

IP Settings

Address Type: Static

IP Address: 172 . 16 . 0 . 1

Subnet Mask: 255 . 255 . 255 . 252

Address Type to be Static, then type in 172.16.0.1 as the IP address with the subnet mask being 255.255.255.252.

Finally, click "Apply" to complete the Demand Interface Configuration. Once completed, there will be one demand interface shown under Add/Delete/Modify Demand Interface.

Assigning a Dial Interface to a Resource Pool

After adding the Demand Interface, it must be associated with a physical interface. In this example, a modem interface is being used. Under Assign Dial Interfaces to a Resource Pool, select the modem 1/1 as the member and the Resource Pool as the pool from earlier in this guide (Backup).

Leave the Priority as 1 as this is the only dial interface currently installed and click add to add modem 1/1 as a resource pool interface.
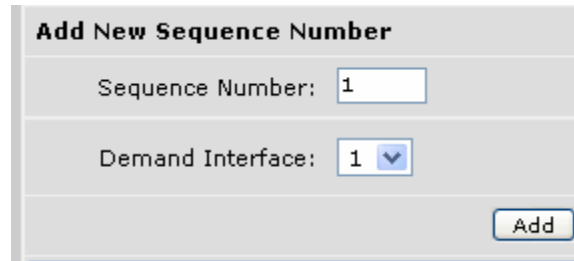
If a resource pool cannot be associated with a dial interface, please verify that the interface is not also being used for remote admin. If in the configuration under this interface you see:
interface modem 1/1
dialin
Please remove this command to allow the interface to be used for routing purposes.

Add Connect Sequences

In this step, phone numbers to dial need to be associated into a sequence so that if one fails, there is another number to failover to. To set a connect sequence, type 1 into the Sequence Number and then select the "Demand Interface" (1) to be used. After selecting this; click add to bring up options for this connect sequence. There are two different types of DBU Modules that can be used. Below is a description for configuring each:
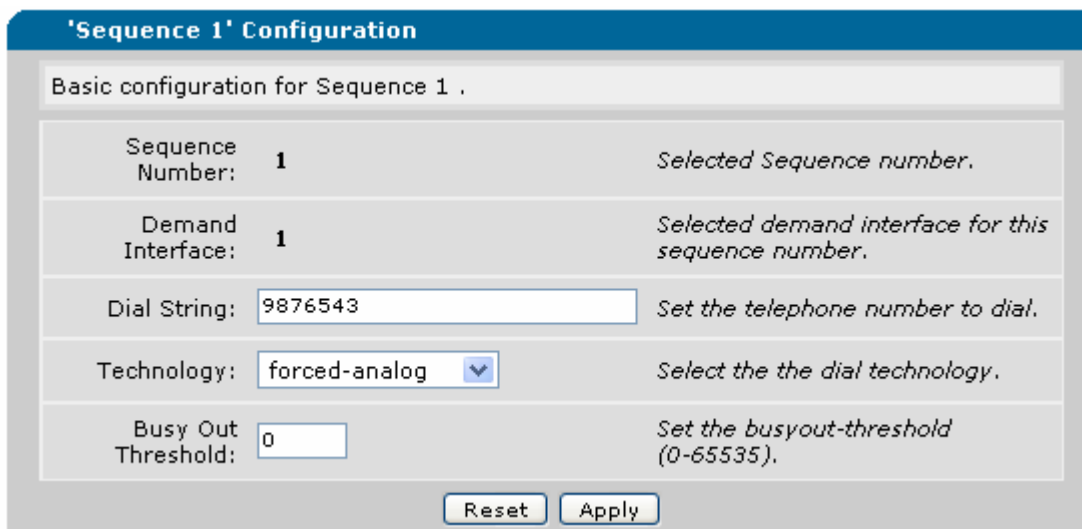
Add New Sequence Number

Sequence Number: `1`

Demand Interface: `1` ▼

`Add`

   A) Analog Module
   B) ISDN BRI Module

A) Under the 'Sequence 1 Configuration,' type in the phone number (Dial String) that will be used to call the remote party. In this case, the number to dial is 9876543. After doing this, select forced-analog as the technology to use since Router A is using an analog modem.

'Sequence 1' Configuration

Basic configuration for Sequence 1 .

Sequence Number:	**1**	Selected Sequence number.
Demand Interface:	**1**	Selected demand interface for this sequence number.
Dial String:	`9876543`	Set the telephone number to dial.
Technology:	`forced-analog` ▼	Select the the dial technology.
Busy Out Threshold:	`0`	Set the busyout-threshold (0-65535).

`Reset` `Apply`

B) Under the 'Sequence 1 Configuration,' type in the phone number (Dial String) that will be used to call the remote party. In this case, the number to dial is 9876543. After doing this, select ISDN-64K as the technology to use since Router A is using an ISDN-64K Circuit as shown below:

'Sequence 1' Configuration

Basic configuration for Sequence 1 .

Sequence Number:	1	Selected Sequence number.
Demand Interface:	1	Selected demand interface for this sequence number.
Dial String:	2569876543	Set the telephone number to dial.
Technology:	isdn-64k	Select the the dial technology.
Busy Out Threshold:	0	Set the busyout-threshold (0-65535).

Reset   Apply

After setting the 'Sequence 1' Configuration, the BRI DBU needs to have SPIDS and LDNs assigned to the interface for the D channel to become active allowing calls to pass. To navigate to this, go to 'Physical Interfaces' under 'System' on the menu at the left of the Web Page as shown to the right.

Once on this page, click on the interface name 'bri 1/1' to open up the configuration page for the BRI DBU module.
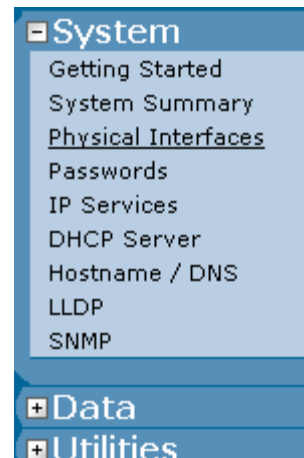
From here, it is important to set the LDNs and SPIDs which should have been provided to you by the provider. An example configuration of one spid configured is shown below:

Configuration for "BRI 1/1"

Basic configuration for the ISDN BRI interface.

Description:		Description label (optional)
Enable:	☑	Enable or disable this interface
Caller-Id Override:	Normal	Caller ID may be replaced with an override number.
Switch-Type:	basic-ni	Switch-type for this interface
LDN1:	2561234567	Primary LDN
LDN2:		Secondary LDN
SPID1:	25612345670101	Primary SPID
SPID2:		Secondary SPID

Reset   Apply

After setting the LDN and SPID information, click apply to finish the configuration of the BRI physical interface.

Add Route Statement

Click on Route Table to add a route for the Demand Interface. Type in 10.10.20.0 as the Destination Network under Add a Static Route to the Route Table with a subnet mask of 255.255.255.0.

Add a Static Route to the Route Table

Static Routes are often required to reach networks that are not learned via a dynamic routing protocol. Enter the appropriate information below to add a static route or click on a route below to use it as a template for a new route. IP Routing must be enabled in order to add static routes.

Destination Address:	10 . 10 . 20 . 0	Enter the network to add to the route table.
Destination Mask:	255 . 255 . 255 . 0	Enter the appropriate mask for this network.

Gateway:

○ Address	[ ] . [ ] . [ ] . [ ]	Enter the gateway address to reach this network. - OR -
⊙ Interface	demand 1 ▼	Select the interface to be used as the gateway.

Finally, click the Add button at the bottom of this box. Since Demand interfaces spoof that they are up even if no traffic is passing across, there should not be a route at the bottom for the 10.10.20.0 network as shown below:

Destination	Mask	Next Hop	Dist	Type	
0.0.0.0	0.0.0.0	10.19.243.254	1	Static	Delete
10.10.10.0	255.255.255.0	0.0.0.0	0	Connected	
10.10.20.0	255.255.255.0	demand 1	1	Static	Delete
10.19.243.0	255.255.255.0	0.0.0.0	0	Connected	
172.16.0.0	255.255.255.252	0.0.0.0	0	Connected	

Once this route has been added, any traffic destined for the 10.10.20.0 subnet should pass through the demand interface.

Saving the Configuration

It is important that you save your configuration!

After you have completed configuring your AOS router, click the 'Save' button in the top right corner.

Save   Logout
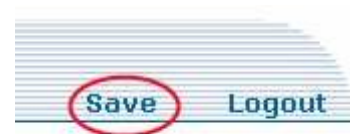
You should also consider downloading the configuration to your desktop. This ensures that you will always have a backup copy of the configuration for your router.

Click 'Configuration' in the left hand menu.
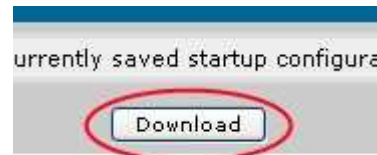
Click 'Download Configuration'. Save this file on your computer, and create backup copies. You can user this file to restore your router to its current settings.

CLI Configuration

For CLI configuration, assume the same network diagram as for the Web Configuration. For reference, the table is shown below:

Setting	Router A*	Router B
Ethernet IP Address	10.10.10.1	10.10.20.1
Ethernet Subnet Mask	255.255.255.0	255.255.255.0
Demand IP Address	172.16.0.1	172.16.0.2
Demand Subnet Mask	255.255.255.252	255.255.255.252
Local Phone Number	1234567	9876543
PPP Authentication	Sending	Authenticating
PPP Username	TEST	TEST
PPP Password	TEST123	TEST123

*Only steps for Router A are shown in this guide.

Gaining Access to Configuration Mode:

It is important to note that after each command, that enter is pressed. If not, the commands will be tied together and will result in an unrecognized command.

Type the command **enable** to access Enable Mode. If you do not know the enable password, consult the document titled "I lost the password to my AOS device".

Type the command **configure terminal** to enter Global Configuration Mode.

Creating List for Interesting Traffic

As is the same with the Web Interface, it is important to first create an access-list to match the traffic that should cause the connection to become active.

Type **ip access-list extended Backup** to create an access-list.

Type **permit ip 10.10.10.0 0.0.0.255 10.10.20.0 0.0.0.255** to create the proper statement to match traffic from one private subnet to the remote subnet. Remember than an access list uses wildcard masks, which are basically inverse subnet masks.

Type **exit** to leave the access-list configuration menu and return to the Global Configuration Mode.

Creating a Demand Interface

The following creates a demand interface that specifies the interesting traffic to match, the number to dial, as well as the PPP interface configuration including IP addressing and Authentication.

Type **interface demand 1** to enter the Demand Interface Configuration Mode.

Type **resource pool backup** to create the resource pool that will associate logical interfaces to our physical dialup interfaces.

Type **match-interesting list Backup out** to match the traffic that will cause this router to originate a call out a dialup interface.

Type **match-interesting reverse list Backup** in to match the traffic that will cause this router to respond to a call originated from a remote device.

Type **connect-sequence 1 dial-string 9876543 forced-analog** to create the first connect sequence to dial if interesting traffic is matched. Note that if there are multiple peers, each can be identified by a different sequence number and then dialed in order (i.e. connect-sequence 2 would be the second number dialed).

Type **connect-sequence attempts 5** to set the number of attempts the modem should use to attempt to connect to the remote location. If this number of attempts is hit, the call is abandoned.

Type **ip address 172.16.0.1 255.255.255.252** to set the IP address of the logical PPP interface that will be created upon call setup.

Type **ppp chap hostname TEST** to set the hostname to be sent for authentication. Then, type **ppp chap password TEST123** to set the password to be sent for CHAP authentication.

Note: If this would have been Router B, instead of setting the chap hostname and password to send, you would have instead set the Demand Interface to use Chap authentication as shown below:

Type **ppp authentication chap** to authenticate remote connections using CHAP.

Type **username TEST password TEST123** to set a username and password to be used to authenticate remote users.

Type **no shutdown** to activate the Demand Interface.

Type exit to leave the Demand Interface Configuration Mode.

Assigning a Dial Interface to a Resource Pool

After adding the Demand Interface, it must be associated with a physical interface. Type **interface modem 1/1** to enter the Modem Interface Configuration Mode.

Type **resource-pool member Backup 1** to set the pool this physical interface should be associated with. The sequence number (1) attached at the end specifies at what point this modem should become active for the resource pool. Since it has a sequence number of 1, it is the first interface to attempt to dial out.

Type **no shutdown** to activate the Modem Interface.

> Note: If this had been an ISDN BRI Module, there would have been additional steps needed. After setting the module to be a member of the resource-pool Backup, and activating the link, you would also need to set the SPIDs that should be used on that link. Below is the command needed to add a SPID to this interface:
> **isdn spid1 25612345670101 2561234567**
> Since there are two data channels, you can have a total of two SPIDs per ISDN BRI module. The second SPID would be created the same as t he first with the only change being **spid2** and the numbers associated with it.

Type **exit** to leave the Modem Interface Configuration Mode.

Add Route Statement

Once the Modem and Demand interface are configured, there needs to be a route statement that tells the router to send traffic destined to the remote network out the Demand Interface.

Type **ip route 10.10.20.0 255.255.255.0 demand 1** to set a router to the 10.10.20.0 network.

After typing this, type **exit** to exit the Global Configuration Mode. Demand interfaces spoof themselves as UP and Active at all times, therefore the route we entered should be listed in the route table.

Type **show ip route** and there should be a route listed for this subnet:

```
Switch#sh ip route
Codes: C - connected, S - static, R - RIP, O - OSPF, B - BGP
     IA - OSPF inter area, N1 - OSPF NSSA external type 1
     N2 - OSPF NSSA external type 2, E1 - OSPF external type 1
     E2 - OSPF external type 2

Gateway of last resort is 10.19.243.254 to network 0.0.0.0

S    0.0.0.0/0 [1/0] via 10.19.243.254, vlan 1
C    10.10.10.0/24 is directly connected, vlan 2
S    10.10.20.0/24 [1/0] via 0.0.0.0, demand 1
```

C   10.19.243.0/24 is directly connected, vlan 1
C   172.16.0.0/30 is directly connected, demand 1
C   172.16.0.2/32 is directly connected, demand 1

Switch#

Saving the Configuration

From the enable (privileged) mode, type **write memory** or **copy running-config startup-config** to copy the running configuration to startup so that it loads upon the next boot.

Example Configuration

hostname "Switch"
enable password password
!
clock timezone -5
!
ip subnet-zero
ip classless
ip routing
!
!
!

!
no ip route-cache express
!
auto-config
!
event-history on
no logging forwarding
no logging email
logging email priority-level info
!
no service password-encryption
!
username "admin" password "password"
!

```
!
ip firewall
no ip firewall alg msn
no ip firewall alg h323
!
!
!
!
!
!
!
!
no dot11ap access-point-controller
!
!
!
!
!
!
!
!
!
!
!
!
!
vlan 1
  name "Default"
!
interface switchport 0/1
  no shutdown
!
interface switchport 0/2
  no shutdown
!
interface switchport 0/3
  no shutdown
!
interface switchport 0/4
  no shutdown
!
```

```
interface switchport 0/5
  no shutdown
!
interface switchport 0/6
  no shutdown
!
interface switchport 0/7
  no shutdown
!
interface switchport 0/8
  no shutdown
!
interface switchport 0/9
  no shutdown
!
interface switchport 0/10
  no shutdown
!
interface switchport 0/11
  no shutdown
!
interface switchport 0/12
  no shutdown
!
interface switchport 0/13
  no shutdown
!
interface switchport 0/14
  no shutdown
!
interface switchport 0/15
  no shutdown
!
interface switchport 0/16
  no shutdown
!
interface switchport 0/17
  no shutdown
!
interface switchport 0/18
```

```
   no shutdown
!
interface switchport 0/19
  no shutdown
!
interface switchport 0/20
  no shutdown
!
interface switchport 0/21
  no shutdown
!
interface switchport 0/22
  no shutdown
!
interface switchport 0/23
  no shutdown
!
interface switchport 0/24
  no shutdown
!
!
interface gigabit-switchport 0/1
  no shutdown
!
interface gigabit-switchport 0/2
  no shutdown
!
!
!
interface vlan 1
  ip address  10.10.10.1  255.255.255.0
  ip route-cache express
  no shutdown
!
!
interface t1 1/1
  clock source internal
  tdm-group 1 timeslots 1-24 speed 64
  no shutdown
!
```

```
interface t1 1/2
  clock source internal
  shutdown
!
interface modem 1/1
  resource pool-member Backup 1
  no shutdown
!
!
interface fr 1 point-to-point
  frame-relay lmi-type ansi
  no shutdown
!
interface demand 1
  fast-idle 120
  resource pool Backup
  match-interesting list Backup out
  match-interesting reverse list Backup in
  connect-sequence 1 dial-string 9876543 forced-analog
  connect-sequence attempts 5
  description Demand 1
  ip address  172.16.0.1  255.255.255.252
  hold-queue 428 out
  ppp chap hostname TEST
  ppp chap password TEST123
  no shutdown
!
!
!
!
!
!
!
ip access-list extended Backup
  permit ip 10.10.10.0 0.0.0.255  10.10.20.0 0.0.0.255    log
!
!
!
ip route 10.10.20.0 255.255.255.0 demand 1
!
```

```
no ip tftp server
no ip tftp server overwrite
ip http server
no ip http secure-server
ip snmp agent
no ip ftp server
ip ftp server default-filesystem flash
no ip scp server
no ip sntp server
!
!
!
!
!
snmp-server community public RO
!
!
!
!
line con 0
  no login
!
line telnet 0 4
  login
  password password
  no shutdown
line ssh 0 4
  login local-userlist
  no shutdown
!
!
!
!
!
end
Switch#
```

Troubleshooting

When troubleshooting a Demand Interface, it is best to test by using debugging information and troubleshooting from the router.

There are essentially three steps to bringing up a demand interface:

1. Send interesting traffic.
2. Establish a call connection.
3. Bring up PPP.

Sent Interesting Traffic

It is possible to attempt to bring up the call from within the router itself. By using the ping utility and specifying the destination to be an IP address on the remote side of the call and the source to be the local IP address on this router, the call should try to establish. Below is an example of what this command would look like for our configuration:

RouterA#ping 10.10.20.1 source 10.10.10.1

The call may take up to a minute to a minute and a half to finish setup so if you only do five pings, all will fail. After it has came up, you will receive the following interface status information:

2007.06.22 08:22:00 PPP.NEGOTIATION modem 1/1: LCP up
2007.06.22 08:22:04 PPP.NEGOTIATION demand 1: LLDPCP up
2007.06.22 08:22:04 PPP.NEGOTIATION demand 1: IPCP up
2007.06.22 08:22:05 INTERFACE_STATUS.demand 1 changed state to up

Now, trying the ping again should result in 5 successful pings.

If you are not sure if the connection is working, do a **show interface demand 1** and a **show interface modem 1/1**. If both of these interfaces show that they are up and demand 1is not spoofing, then you should be able to pass traffic across this connection.

Establish a Call Connection

Sometimes there is a need to debug a connection that seems not to come up. Use the following three commands to troubleshoot a bad connection as it is possible to monitor the call as it becomes active:

debug dialup-interfaces
debug dial-backup
debug demand-routing

The following is the most likely result of a bad phone call:

2007.06.22 08:49:34 DEMANDROUTING.Demand Interface Demand 1 interesting traffic packet saved
2007.06.22 08:49:34 DEMANDROUTING.Demand Interface Demand 1 dialing
2007.06.22 08:49:36 DIALUP_INTERFACE.modem 1/1 Dialing 9876542
2007.06.22 08:49:43 DIALUP_INTERFACE.modem 1/1 ATDT9876542.BUSY

If you do receive this message, first, check and make sure that the far end has not already answered a phone call. Then, verify that the other end is configured correctly and can receive phone calls. Finally, check the settings on the local Adtran and make sure that it is dialing the correct number. If a phone is present, attempt to dial the remote modem from a phone and make sure that you receive dial-tone.

Bring Up PPP

If the call is successful, the next step in passing traffic is to establish the PPP link. To troubleshoot this link, there are two commands that can be helpful:

debug ppp negotiation
debug ppp authentication

Debug ppp authentication will not be helpful unless there is authentication on the link, but it is the only way to verify that the username and password are correct.

Below is an example of when authentication parameters do not match (I.E. we send PAP authentication when it should be CHAP):

2007.06.22 12:58:57 PPP.NEGOTIATION PPPtx[modem 1/1] LCP: Conf-Req ID=1 Len=16
ACCM(000a0000) MAGIC(f666154a)
2007.06.22 12:58:57 PPP.NEGOTIATION PPPrx[modem 1/1] LCP: Conf-Req ID=1 Len=21
ACCM(000a0000) AP(CHAP)MAGIC(efaa0334)
2007.06.22 12:58:57 PPP.NEGOTIATION PPPtx[modem 1/1] LCP: Conf-Nak ID=1 Len=8 AP(PAP)

As you can see from the above debug, we are receiving a request for CHAP, but we are sending a username of PAP. Changing our settings to send CHAP will resolved this issue.

Another problem is the username being incorrect, below is an example of what would occur if this was the case:

2007.06.22 13:06:07 PPP.NEGOTIATION modem 1/1: LCP up
2007.06.22 13:06:07 PPP.AUTHENTICATION PPPrx[modem 1/1] CHAP: Challenge ID=1 Len=27
ValLen=16 Name(Switch)
2007.06.22 13:06:07 PPP.AUTHENTICATION PPPtx[modem 1/1] CHAP: Response ID=1 Len=24
ValLen=16 Name(TES)n
2007.06.22 13:06:07 PPP.AUTHENTICATION PPPrx[modem 1/1] CHAP: Failure ID=1 Len=4
Message()
2007.06.22 13:06:07 PPP.NEGOTIATION modem 1/1:

In this case, it appears that the username and/or password are incorrect as the fourth message shows us that CHAP failed. To remedy this, double check the other end and verify that the username and password match.

I have done all of the above troubleshooting, but I am still unable to ping.

Please double check the default gateway settings of the computers connected to the private networks. Either the PC needs to have it's default gateway as the NetVanta with the Demand Interface or it needs to have a route to that network.
[[ArticleBody:User1-optional,optional]]

If you experience any problems using your ADTRAN product, please contact ADTRAN Technical Support.