NetVanta Series
(with Octal T1/E1 Wide Module)

Quick Configuration Guide 61202843L1-42A November 2005

Before You Begin

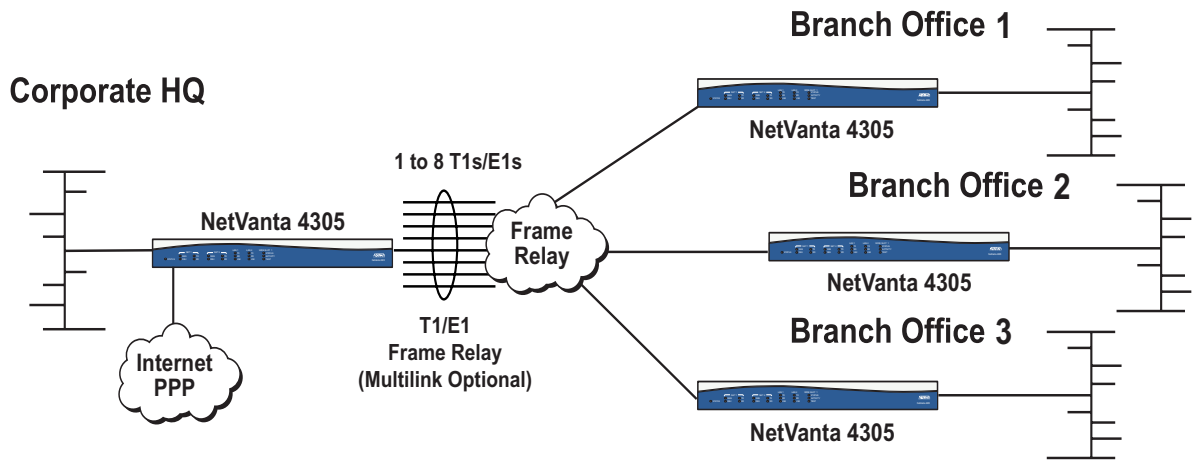
This quick configuration guide assumes that you have already connected to the NetVanta by following the instructions in the *Quick Start Guide* provided with your unit.

NOTE

This quick configuration guide provides step-by-step instructions for configuring the example application.

The configuration parameters used in the example outlined in this document are for instructional purposes only. Please use your specific parameters to configure your application.

Network Diagram



In the example network shown above, a corporate office provides centralized Internet access for three branch offices. Each branch is connected back to the corporate office using a Frame Relay link. The public Internet connection at the corporate office is provided using a point-to-point (PPP) connection to the Internet service provider (ISP). Refer to the following chart for configuration parameters required for this example.

Configuration Parameter Chart

Parameter	Corporate HQ	Branch 1	Branch 2	Branch 3
WAN Interface(s)	t1 3/1 (1-24) t1 3/2 (1-24) t1 3/3 (1-24)	t1 1/1 (1-24)	t1 1/1 (1-24)	t1 1/1 (1-24)
LAN: Eth 0/1 IP	10.10.0.7/24	10.10.10.1/24	10.10.20.1/24	10.10.30.1/24
Frame Relay Interface(s)	fr 1.16 fr 1.17 fr 1.18	fr 1.19	fr 1.20	fr 1.21
DLCI	16 17 18	19	20	21
Signaling Type	Annex D	Annex D	Annex D	Annex D
IP Address	192.168.72.1/30 192.168.72.5/30 192.168.72.9/30	192.168.72.2/30	192.168.72.6/30	192.168.72.10/30
Internet Connection	t1 3/8 (1-18)	N/A	N/A	N/A
PPP Interface	ppp 1			
IP Address	68.22.15.2/30			

Configuration Overview

Configuring the example network consists of the following steps:

1. Configure the physical interfaces (Ethernet and WAN interfaces)
2. Configure the Layer 2 (L2) protocol(s)
3. Cross-connect the physical and virtual (L2) interfaces
4. Create access lists and policies (including NAT parameters)
5. Apply the policies to interfaces
6. Configure the routing information (static routes, OSPF, RIP, etc.)

This document outlines the procedures for completing each of the steps listed above. In addition to the commands required to configure the sample network, each configuration step provides a brief discussion of available settings, but does not elaborate on parameters that are normally left in the default state. For detailed information regarding wide area network (WAN) configuration parameters, refer to the supplemental documentation provided on your *ADTRAN OS System Documentation* CD.

Configure the Physical Interfaces

To begin configuring physical interfaces, you must first activate the appropriate interface configuration mode from the Global Configuration mode prompt. For example, enter the following commands to activate the interface configuration mode for the first T1 interface on the Octal T1/E1 Wide Module:

>**enable**
#configure terminal
(config)**#interface t1 3/1**
(config-t1 3/1)**#**

> NOTE *The NetVanta Network Interface Modules (NIMs) use a* **slot/port** *notation for interface identification. All non-modular interfaces built into the base unit (e.g., the Ethernet ports) are identified using* **0** *as the slot number.*

Configuring the Ethernet Interface(s)

Ethernet interface configuration can range from assigning an IP address and activating the interface to activating the Dynamic Host Configuration Protocol (DHCP) client to poll the network DHCP server to gain an IP address. Standard Ethernet configurations generally contain an IP address, a speed, and a duplex setting. By default, all NetVanta Ethernet interfaces are configured to automatically detect the speed (as 10 or 100 Mbps) and are set to full-duplex. For most cases, these settings should suffice and will not be changed from the default state.

The following command listing configures the IP address (10.10.0.7/24) and activates the interface for the Corporate Router eth 0/1 interface:

>**enable**
#configure terminal
(config)**#interface eth 0/1**
(config-eth 0/1)**#ip address 10.10.0.7 255.255.255.0**
(config-eth 0/1)**#no shutdown**
(config-eth 0/1)**#exit**
(config)#

Configure each of the branch sites in the same manner by replacing the IP address with one appropriate for the location.

Configuring the T1/E1 Interface(s)

There are four main settings to consider when configuring T1/E1 network interfaces. The line coding (**coding**), framing format (**framing**), active channels (**tdm-group**), and clock source (**clock source**) must all be configured to match the circuit supplied by your network provider. By default, all NetVanta T1 interfaces are configured for ESF (**framing esf**) and B8ZS (**coding b8zs**), and to recover clocking from the network circuit (**clock source line**). By default, all NetVanta E1 interfaces are configured for standard multiframe without the optional CRC-4 error

correction (**no framing crc4**), and to recover clocking from the network circuit (**clock source line**). Generally, the line coding, framing format, and clock source default values will be the correct ones for your application and should not be changed. Each configured T1/E1 interface must have the active channels specified using the **tdm-group** command because there are no default TDM groups. The active channels are entered as a single number representing 1 of the 24 (T1) or 31 (E1) channel timeslots or as a contiguous group of channels.

The following command listing specifies the configuration parameters required for the Corporate Router T1 (or E1) interfaces:

>**enable**
#configure terminal
(config)**#interface t1 3/1**
(config-t1 3/1)**#tdm-group 1 timeslots 1-24**
(config-t1 3/1)**#no shutdown**
(config-t1 3/1)**#exit**

(config)**#interface t1 3/2**
(config-t1 3/2)**#tdm-group 2 timeslots 1-24**
(config-t1 3/2)**#no shutdown**
(config-t1 3/2)**#exit**

(config)**#interface t1 3/3**
(config-t1 3/3)**#tdm-group 3 timeslots 1-24**
(config-t1 3/1)**#no shutdown**
(config-t1 3/3)**#exit**

(config)**#interface t1 3/8**
(config-t1 3/8)**#tdm-group 4 timeslots 1-18**
(config-t1 3/1)**#no shutdown**
(config-t1 3/8)**#exit**

Configure each of the Branch sites in the same manner using the appropriate T1 slot and port and active channels for the location.

Configure the L2 Protocol(s)

To begin configuring the L2 protocol(s), first determine whether you need to configure Frame Relay, PPP, or high-level data link control (HDLC). Each L2 protocol has unique configuration specifications. For the purpose of this guide, we will briefly discuss Frame Relay and PPP.

Configuring the Frame Relay Interfaces (and Sub-Interfaces)

There are two settings to consider when configuring Frame Relay interfaces. The interface type (**frame-relay intf-type**) and signaling type (**frame-relay lmi-type**) must be configured to match the specifications supplied by your network provider. By default, all NetVanta Frame Relay interfaces are configured as a data terminal equipment (DTE) interface (**frame-relay intf-type dte**) with Annex D signaling (**frame-relay lmi-type ansi**). Multilink operation is also configured in the Frame Relay interface using the **frame-relay multilink** command.

Frame Relay interfaces have a sub-interface component for each permanent virtual circuit (PVC) which must also be configured. Each Frame Relay sub-interface contains a data link correction identifier (DLCI) (**frame-relay interface-dlci**) and IP address (**ip address**). You must manually configure the Frame Relay sub-interface DLCI and IP address because there are no default DLCIs or IP addresses defined. Access policies are also applied at the sub-interface level (but these are discussed later in this document). Each PVC should also have a configured committed burst value (**frame-relay bc**) (equivalent to the committed information rate (CIR) given to you by your network provider) and a negotiated burst rate (**frame-relay be**) (equivalent to the excess information rate (EIR) given to you by your network provider). Both the CIR and EIR should be decided on by you and your service provider when defining your service agreement. To determine the appropriate committed burst value and EIR, you need to know the CIR and physical bandwidth for both the local and remote connections. If one side transmits data at a rate much higher than the other side's CIR (or physical bandwidth), packets will be dropped, causing a decrease in efficiency. A general rule is to provision the committed burst value with the remote side CIR and configure the EIR with the difference between the CIR and the actual physical bandwidth at the location. The committed burst value plus the EIR should not be greater than the physical bandwidth.

The following command listing specifies the configuration parameters required for the corporate router Frame Relay interface:

>**enable**
#configure terminal
(config)**#interface fr 1**
(config-fr 1)**#frame-relay multilink**
(config-fr 1)**#no shutdown**
(config-fr 1)**#exit**

The following command listing specifies the configuration parameters required for the corporate router Frame Relay sub-interfaces:

(config)**#interface fr 1.16**
(config-fr 1.16)**#frame-relay interface-dlci 16**
(config-fr 1.16)**#frame-relay bc 768000**
(config-fr 1.16)**#frame-relay be 768000**
(config-fr 1.16)**#ip address 192.168.72.1 /30**
(config-fr 1.16)**#no shutdown**
(config-fr 1.16)**#exit**

(config)**#interface fr 1.17**
(config-fr 1.17)**#frame-relay interface-dlci 17**
(config-fr 1.17)**#frame-relay bc 768000**
(config-fr 1.17)**#frame-relay be 768000**
(config-fr 1.17)**#ip address 192.168.72.5 /30**
(config-fr 1.17)**#no shutdown**
(config-fr 1.17)**#exit**

(config)**#interface fr 1.18**
(config-fr 1.18)**#frame-relay interface-dlci 18**
(config-fr 1.18)**#frame-relay bc 768000**
(config-fr 1.18)**#frame-relay be 768000**
(config-fr 1.18)**#ip address 192.168.72.9 /30**
(config-fr 1.18)**#no shutdown**
(config-fr 1.18)**#exit**

> NOTE *Labeling the Frame Relay sub-interfaces using the DLCI (such as* **1.16** *indicating a DLCI of 16) is useful for quickly determining (from a configuration printout) which sub-interface corresponds to which PVC.*

The Frame Relay interfaces and sub-interfaces for each branch site are configured in the same manner.

Configuring the PPP Interface

There are two settings to consider when configuring PPP interfaces: the IP address and the maximum transmission unit (MTU). There are no default IP addresses, so each interface must be manually programmed with the appropriate address (**ip address**). All NetVanta PPP interfaces have a default MTU of 1500 bytes, which works for most applications.

Multilink PPP is also configured on the PPP interface (using the **ppp multilink** command).

The following command listing specifies the configuration parameters required for the corporate router PPP interface:

```
>enable
#configure terminal
(config)#interface ppp 1
(config-ppp 1)#ip address 68.22.15.2 /30
(config-ppp 1)#no shutdown
(config-ppp 1)#exit
(config)#
```

Cross-Connect the Physical and Virtual (L2) Interfaces

Virtual interfaces must be cross connected to physical interfaces to create a WAN interface where L2 signaling occurs. Use the **cross-connect** command to connect the physical and virtual interfaces together. A single virtual interface is assigned to a single physical interface, except in the case of multilink operation, where one virtual interface is connected with multiple physical interfaces. Each created cross connect has a unique label identifier and specifies a virtual and a physical interface.

The following command listing specifies the cross connects required to complete the WAN interface configuration for the corporate router:

>**enable**
#configure terminal
(config)**#cross-connect 1 t1 3/1 1 fr 1**
(config)**#cross-connect 2 t1 3/2 2 fr 1**
(config)**#cross-connect 3 t1 3/3 3 fr 1**
(config)**#cross-connect 4 t1 3/8 4 ppp 1**

Cross connects are configured in the same manner for each branch site.

Create the Access Lists and Policies

Access lists (ACLs) and access policies (ACPs) are used to regulate traffic through your routed network. ACLs and ACPs can block, filter, and manipulate traffic to make your network more secure.

ACLs are traffic selectors that include a “matching” parameter (to select the traffic) and an action statement (to either permit or deny the matched traffic). Standard ACLs (using the **ip access-list standard** command) provide pattern matching for source IP addresses only. Use extended ACLs (using the **ip access-list extended** command) for more flexible pattern matching (including destination IP addresses).

ACPs use configured ACLs to permit, deny, or manipulate (using NAT) data on each interface where the ACP is applied. When packets are received on an interface, the configured ACPs are applied to determine whether the data will be processed or discarded. Creating access policies is a five-step process:

1. Determine what traffic needs to be regulated
2. Enable the security feature (using the **ip firewall** command)
3. Create an ACL to act as a traffic selector
4. Create an ACP to either permit, deny, or manipulate (using NAT) the traffic selected using an access list
5. Apply the ACP to an interface (or multiple interfaces)

For our example, evaluate the incoming and outgoing traffic on all the interfaces (**fr 1**, **eth 0/1**, and **ppp 1**). Use ACLs and ACPs to provide connectivity for traffic between all the private local area networks (LANs) (branch sites and corporate headquarters), grant access to the public Internet connection for all users (branch sites and corporate headquarters), and restrict inbound access from the public domain over the PPP and Frame Relay connections to protect the network. The following table outlines our traffic concerns:

Public Interface	Traffic to Select
fr 1	Traffic from remote LANs (10.10.10.0/24, 10.10.20.0/24, and 10.10.30.0/24) to local LAN (10.10.10.0/24)
	Traffic from remote LANs (10.10.10.0/24, 10.10.20.0/24, and 10.10.30.0/24) to the public Internet through the **ppp 1** interface
eth 0/1	Traffic to the remote LANs (10.10.10.0/24, 10.10.20.0/24, and 10.10.30.0/24)
	Traffic to the public Internet through the **ppp 1** interface

Begin by planning the ACL selectors for the traffic received on **fr 1**. Use extended ACLs for source and destination IP addresses to sort the traffic received on **fr 1** from the remote LANs into two categories – traffic destined for other LANs or traffic destined for the public Internet. Each category requires an extended ACL to select the appropriate traffic. All traffic destined for the public Internet requires a many-to-one network address translation (NAT) configuration.

Next, plan the ACL selectors for the traffic received on the **eth 0/1** interface (the corporate LAN). Use extended ACLs for source and destination IP addresses to sort the traffic received on **eth 0/1** into two categories – traffic destined for other LANs or traffic destined for the public Internet. Each category requires an extended ACL to select the appropriate traffic. All traffic destined for the public Internet requires a many-to-one NAT configuration.

The following table provides sample ACL commands for the various traffic on our sample network.

Action	Description	Command(s)
Allow	Traffic between LANs (10.10.0.0/16)	**permit ip 10.10.0.0 0.0.255.255 10.10.0.0 0.0.255.255**
Allow	All traffic from remote LANs (10.10.0.0/16) to the Internet through the **ppp 1** interface	**permit ip 10.10.0.0 0.0.255.255 any**
Allow	Traffic from corporate LAN (10.10.0.0/16) to remote LANs (10.10.0.0/16)	**permit ip 10.10.0.0 0.0.255.255 10.10.0.0 0.0.255.255**
Allow	Traffic from corporate LAN (10.10.0.0/24) to the Internet through the **ppp 1** interface	**permit ip 10.10.0.0 0.0.255.255 any**

The traffic selectors required for traffic on the **fr 1** and **eth 0/1** interfaces are identical. Therefore, we can create a single set of ACLs that can be used in multiple ACPs on multiple interfaces.

The following activates the security features in the NetVanta and creates two extended ACLs to select our traffic:

>**enable**
#configure terminal
(config)**#ip firewall**
(config)**#ip access-list extended INTERLAN**
(config-ext-nacl)**#permit ip 10.10.0.0 0.0.255.255 10.10.0.0 0.0.255.255**
(config-ext-nacl)**#exit**
(config)**#ip access-list extended INTERNET**
(config-ext-nacl)**#permit ip 10.10.0.0 0.0.255.255 any**
(config-ext-nacl)**#exit**
(config)#

Now, create the access policy to allow the traffic between the LANs and NAT traffic bound for the public Internet.

(config)**#ip policy-class INTERLANwNAT**
(config-policy-class)**#allow list INTERLAN**
(config-policy-class)**#nat source list INTERNET interface ppp 1 overload**
(config-policy-class)**#exit**
(config)#

Apply the ACPs to the interface(s) to complete the configuration. For our example, the **INTERLANwNAT** ACP should be applied to the **fr 1** and **eth 0/1** interfaces.

The following command listing applies the ACP to the **fr 1** and **eth 0/1** interfaces:

>**enable**
#configure terminal
(config)**#interface fr 1**
(config-fr 1)**#access-policy INTERLANwNAT**
(config-fr 1)**#exit**
(config)**#interface eth 0/1**
(config-eth 0/1)**#access-policy INTERLANwNAT**
(config-eth 0/1)**#exit**
(config)#

ACLs and ACPs are configured in the same manner for each branch site, but the many-to-one NAT is not required. The NAT operation should be handled by the router with the public connection.

Configure the Routing Information

AOS products support various routing protocols including static routes, RIP, OSPF, and BGP. RIP, OPSF, and BGP are all routing protocols that allow routers to share the information contained in their route tables with other routers in the network. These routing protocols are generally used on networks that frequently change, or contain a large number of nodes. For small applications (such as our example network), manually adding static routes to the router's route table is the easiest method of configuration.

Manually adding static routes to the route table requires two steps:

1. Determine the routes needed (destination address and subnet mask as well as the next-hop address or forwarding interface). Be sure to plan the default route.
2. Use the **ip route** command to add the route to the route table.

The following table outlines the static routes needed in the corporate router.

Destination Address	Subnet Mask	Next-Hop Address/Forwarding Interface
10.10.10.0	255.255.255.0	fr 1.16
10.10.20.0	255.255.255.0	fr 1.17
10.10.30.0	255.255.255.0	fr 1.18
Default Route (0.0.0.0)	0.0.0.0	ppp 1 (public Internet)

The following command listing adds the necessary static routes to the corporate router's route table:

>**enable**
#configure terminal
(config)**#ip route 10.10.10.0 255.255.255.0 fr 1.19**
(config)**#ip route 10.10.20.0 255.255.255.0 fr 1.20**
(config)**#ip route 10.10.30.0 255.255.255.0 fr 1.21**
(config)**#ip route 0.0.0.0 0.0.0.0 ppp 1**
(config)#

Each of the branch sites will need a route to the corporate LAN (10.10.0.0/24) and a default route set as the Frame Relay interface connection back to the corporate router.