



---

Vanguard Applications Ware  
Multi-Service Feature Protocols

Virtual Private Network (VPN)

# Notice

---

©2005 Vanguard Networks  
25 Forbes Blvd  
Foxboro, MA 02035  
USA  
Phone: (508) 964 6200  
Fax: (508) 543 0237  
All rights reserved  
Printed in U.S.A.

## **Restricted Rights Notification for U.S. Government Users**

---

The software (including firmware) addressed in this manual is provided to the U.S. Government under agreement which grants the government the minimum “restricted rights” in the software, as defined in the Federal Acquisition Regulation (FAR) or the Defense Federal Acquisition Regulation Supplement (DFARS), whichever is applicable.

If the software is procured for use by the Department of Defense, the following legend applies:

### **Restricted Rights Legend**

Use, duplication, or disclosure by the Government  
is subject to restrictions as set forth in  
subparagraph (c)(1)(ii) of the  
Rights in Technical Data and Computer Software  
clause at DFARS 252.227-7013.

If the software is procured for use by any U.S. Government entity other than the Department of Defense, the following notice applies:

### **Notice**

Notwithstanding any other lease or license agreement that may pertain to, or accompany the delivery of, this computer software, the rights of the Government regarding its use, reproduction, and disclosure are as set forth in FAR 52.227-19(C).

Unpublished - rights reserved under the copyright laws of the United States.

## Notice (continued)

---

### Proprietary Material

---

Information and software in this document are proprietary to Vanguard Networks, LLC (or its Suppliers) and without the express prior permission of an officer, may not be copied, reproduced, disclosed to others, published, or used, in whole or in part, for any purpose other than that for which it is being made available. Use of software described in this document is subject to the terms and conditions of the Software License Agreement.

This document is for information purposes only and is subject to change without notice.

Part No. T0103-10, Rev L  
Publication Code: TK  
First Printing: September 2000

Manual is current for Release 7.3 of Vanguard Applications Ware.

To comment on this manual, please send e-mail to [vntechsupport@vanguardnetworks.com](mailto:vntechsupport@vanguardnetworks.com)



## Chapter 1.

---

### Virtual Private Network

What is a VPN .....	1-2
VPN Applications .....	1-3

## Chapter 2.

---

### Tunneling

Vanguard VPN Tunneling .....	2-4
Processing .....	2-5
Dynamic Tunnel Address .....	2-8
How does Dynamic Tunnel Address work? .....	2-9
Configuration Examples .....	2-11
Dynamic Tunnel Address Statistics .....	2-16
RTP/UDP/IP Header Compression of Tunneled Packets .....	2-19
Generic Routing Encapsulation (GRE) .....	2-20
Next Hop Resolution Protocol (NHRP) .....	2-23
Tunnel Configuration .....	2-24
Configuration Examples .....	2-32
Tunnel Boot .....	2-40
Statistics .....	2-41

## Chapter 3.

---

### IP Security

Vanguard IP Security .....	3-3
IPSec Configuration .....	3-6
IPSec Configuration Example .....	3-17
GRE_IPSec Example .....	3-19
ISAKMP Aggressive Mode .....	3-21
Statistics .....	3-25
SNMP IPSec Statistics .....	3-31

## Chapter 4.

---

### Digital Certificates and SCEP

X.509 Digital Certificate .....	4-2
Simple Certificate Enrollment Program (SCEP) .....	4-4
Applications and Solutions Support .....	4-6
Detailed Functional Description .....	4-7
Configuration Menu .....	4-10
Configuration .....	4-11
Certificate Management .....	4-18
CA Configuration .....	4-21
IPSec Configuration .....	4-23

## **VPN Technical Glossary**

# Chapter 1

## Virtual Private Network

---

### Overview

#### Introduction

---

This document describes the implementation of the Virtual Private Network (VPN) feature in Vanguard Networks' Vanguard products. VPN includes:

- Tunneling
- Generic Routing Encapsulation (GRE)
- IPSEC
- Digital Certificates and SCEP

#### What's In This Manual?

---

This manual provides a general description of a VPN, tunneling, GRE, IPSEC, Digital Certificates and SCEP and encryption. A detailed description of Vanguard Networks implementation of a VPN, tunneling, GRE, and IPSEC, along with explanations of how to configure Vanguard products to support this feature, are included.

Data encryption information and supported encryption types are explained in detail in the *Data Encryption* manual, (Part Number T0103-09).

#### Terminology

---

Refer to the VPN Technical Glossary located in the back of this manual for the definition of terms specific to the VPN feature.

---

## What is a VPN

---

### Introduction

A Virtual Private Network (VPN) is a network that has the appearance and many of the advantages of a dedicated link but occurs over a shared network. Using a technique called “tunneling,” packets are transmitted across a public routed network, such as the Internet or other commercially available network, in a private “tunnel” that simulates a point-to-point connection. This approach enables network traffic from many sources to travel through separate tunnels across the same infrastructure. VPN allows network protocols to traverse incompatible infrastructures. VPN also enables traffic from many sources to be differentiated, so that it can be directed to specific destinations and receive specific levels of service.

---

### Advantages of a VPN

A VPN provides following advantages:

- Cost Effectiveness
    - *Infrastructure Cost* - By using a VPN, a company need not invest money on connectivity equipment like leased lines, WAN switches etc. The connectivity is provided by the service provider.
    - *Operational Cost* - Costs involved with maintaining leased lines or a private WAN along with the money spent on people to maintain them can be avoided.
  - Manageability
    - A VPN is more easily managed when compared to a fully private network.
- 

### Requirements of a VPN

Below are some of the requirements of a VPN:

- Connectivity
    - There needs to be network connectivity among the various corporate sites. This connectivity is typically used through the Internet.
  - Security
    - Data exchanged between the various corporate sites is confidential. When data is sent over a public network it is usually encrypted. The encryption algorithm must be robust enough to withstand any type of snooping.
  - Address Management
    - The Addresses of the clients on each of the private sites should not be the ones used in the public domain, however, packets sent out onto the public network must have public source/destination addresses.
  - Multiprotocol Support
    - The solution must be able to handle common protocols used in the corporate network.
-

## VPN Applications

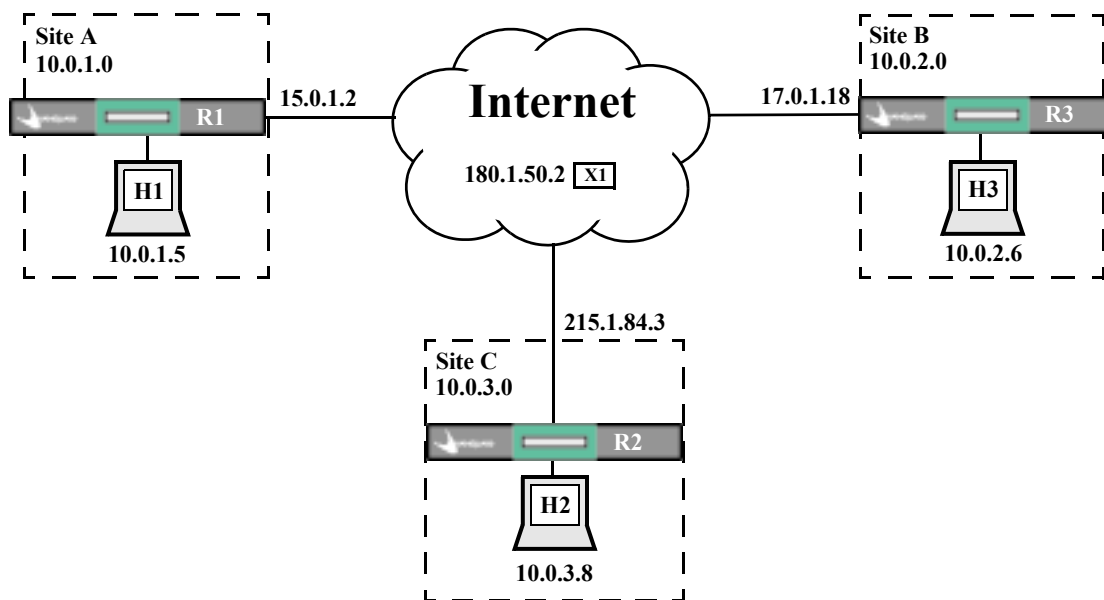
### Tunneling and Address Translation

Figure 1-1 shows a network diagram of a company that has three sites (A, B, and C) connected to the Internet. The Internet has assigned 15.0.1.2 to Site A, 17.0.1.18 to Site B and 215.1.84.3 to Site C. The company is using 10.0.x.x as its private IP address space. Each site is given a distinct IP subnet address from 10.0.x.x.

- It is required that any host in any site (example H1) should be able to communicate with any host (example X1) in the Internet.
- It is required that any host (example H1) should be able to communicate with any other host (example H2) in any of the company's sites using the destination's private address. i.e. H1 should be able to communicate with H2 using H2's private address 10.0.3.8.

The above requirements can be met by using following solutions:

- NAT can be enabled on the interfaces which are connected to the Internet. When the packet from H1 reaches R1 and is destined for X1, R1 translates the source address 10.0.1.5 to 15.0.1.2 and sends it to X1 and does destination address translation when a reply comes back from X1.
- Three tunnels can be established between R1 to R2, R2 to R3 and R1 to R3. When a packet is sent from H1 to H2, the original packet is tunneled by appending a tunnel header and an IP header. The new IP header uses the public address 15.0.1.2 as source address and 215.1.84.3 as destination address. When the tunneled packet reaches R2, the packet is decapsulated and the original packet is sent to H2.



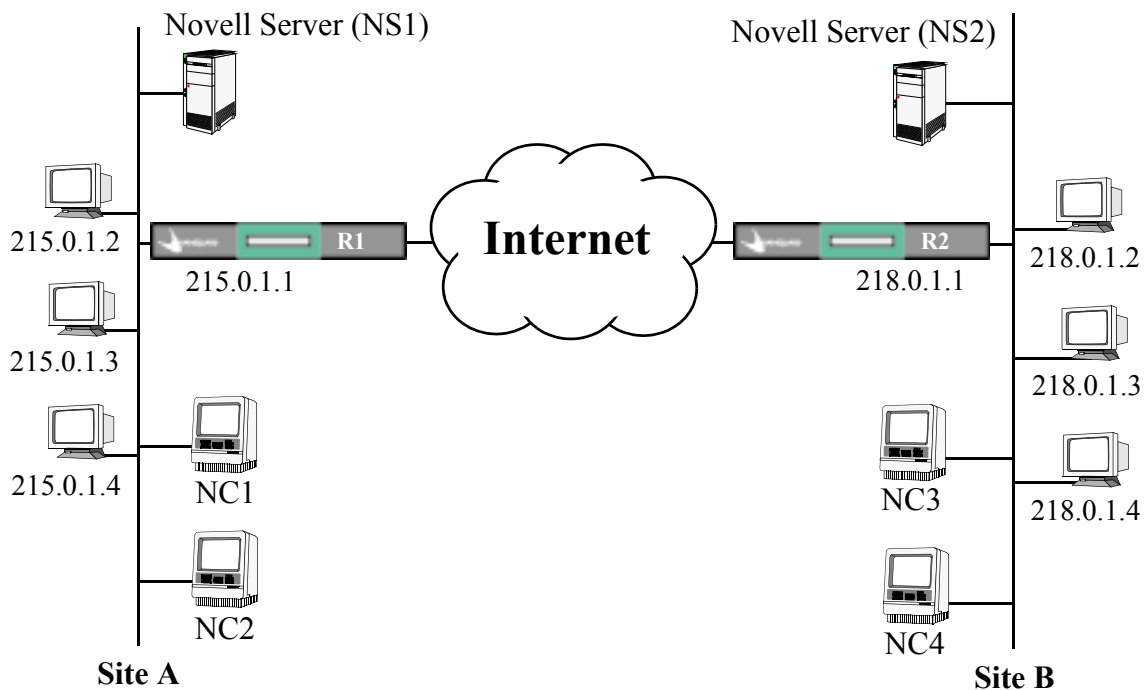
**Figure 1-1. Tunneling and Address Translation**

### Transporting IPX over IP

Figure 1-2 shows how both IP and IPX subnets are operating on the same physical network, on both sites A and B.

In this example, IPX traffic is tunneled through IP and sent without any translation. The overall characteristics of this network are:

- IP hosts are assigned IP addresses.
- Routers R1 and R2 operate both IP and IPX.
- A tunnel is configured between Routers R1 and R2.
- IPX static routes are configured on R1 so that any IPX traffic destined for site B is sent to the tunnel.
- R1 adds the tunnel header and IP header and sends it to Router R2.
- Router R2 removes the IP header and tunnel header and forwards the original IPX packet appropriate IPX host.



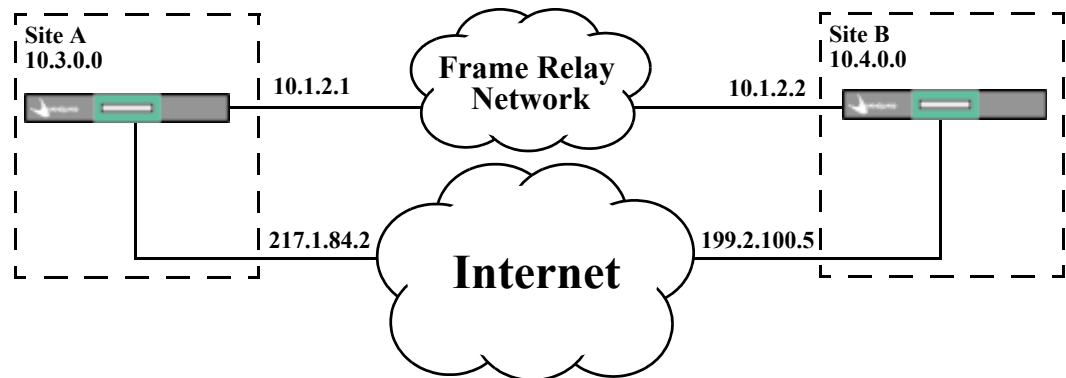
**Figure 1-2. Multiprotocol Traffic**

### Backup through the Internet

Figure 1-3 shows an example of the back up of an inter-site connection through the Internet. Listed below are the sequence of events:

- Site A and Site B are part of a private network having a private network address 10.3.0.0. Site A is assigned 10.1.0.0 and Site B 10.4.0.0.
- Site A and Site B are connected through a Frame Relay network. This link is a subnet having subnet id 10.1.2.0. This is a primary link and all the inter-site traffic goes through this link.

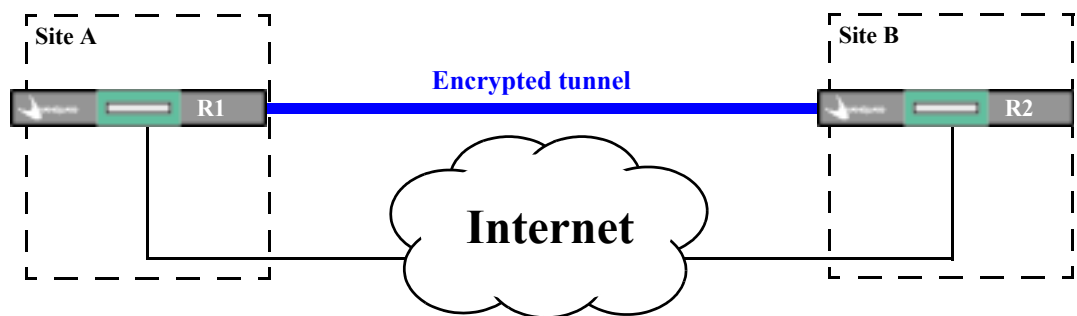
- These sites are also connected via the Internet. The Internet has assigned public network addresses 217.1.84.2 and 199.2.100.5 to Site A and Site B. A tunnel is configured between Site A and Site B through the Internet.
- A static route is configured using the tunnel as the next hop with a higher metric.
- When the Frame Relay network goes down, the route through 10.1.2.1 becomes unreachable. The router module searches the next best route available. Since the static route through the tunnel is available, it is selected. All the traffic going through the Frame Relay network is sent over the tunnel.
- When the Frame Relay network comes back up, the route through 10.1.2.1 again becomes reachable. Since the metric for the route is lower than the metric for the tunnel all traffic is sent over the Frame Relay network and the tunnel is not used.



**Figure 1-3. Backup through the Internet**

**Tunnel Encryption** Figure 1-4 shows an example of how to encrypt only the traffic between Sites A and B. Listed are the sequence of events:

- Site A and Site B are two branches of the same company. Both the sites are connected to the Internet and both use public IP addresses.
- The user wants to encrypt only the traffic between Site A and Site B. A tunnel is created between R1 and R2 and the traffic between R1 and R2 is encrypted.
- All other Internet traffic is not encrypted.

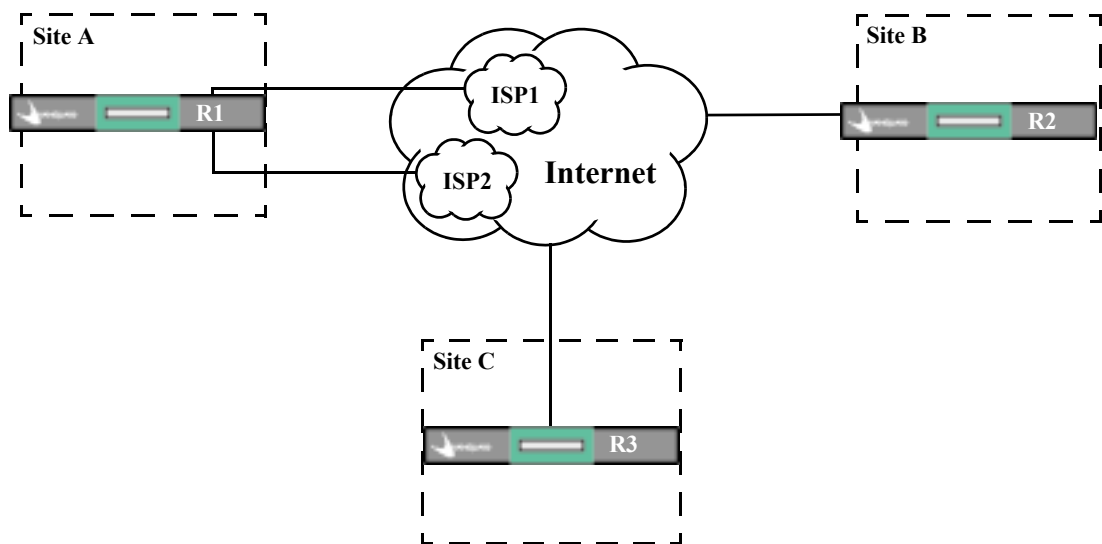


**Figure 1-4. Tunnel Encryption**

**Tunnel Level Backup**

Figure 1-5 shows an example of three sites connected to the Internet. Traffic between all sites is tunneled. R1 has two connections to the Internet via ISP1 and ISP2. Here is the sequence of events:

- A tunnel is configured between R1 and R2 via ISP1.
- A tunnel is configured between R1 and R3 via ISP2.
- A backup tunnel (through static routes with a higher metric) is configured between R1 and R2 via ISP2.
- A backup tunnel (through static routes with a higher metric) is configured between R1 and R3 via ISP1.
- When the connection to ISP1 fails, traffic from R1 to R2 is sent over ISP2.
- When the connection to ISP2 fails, traffic from R1 to R3 is sent over ISP1.



**Figure 1-5. Tunnel Level Backup**

## Tunnel Support for Bridge Traffic

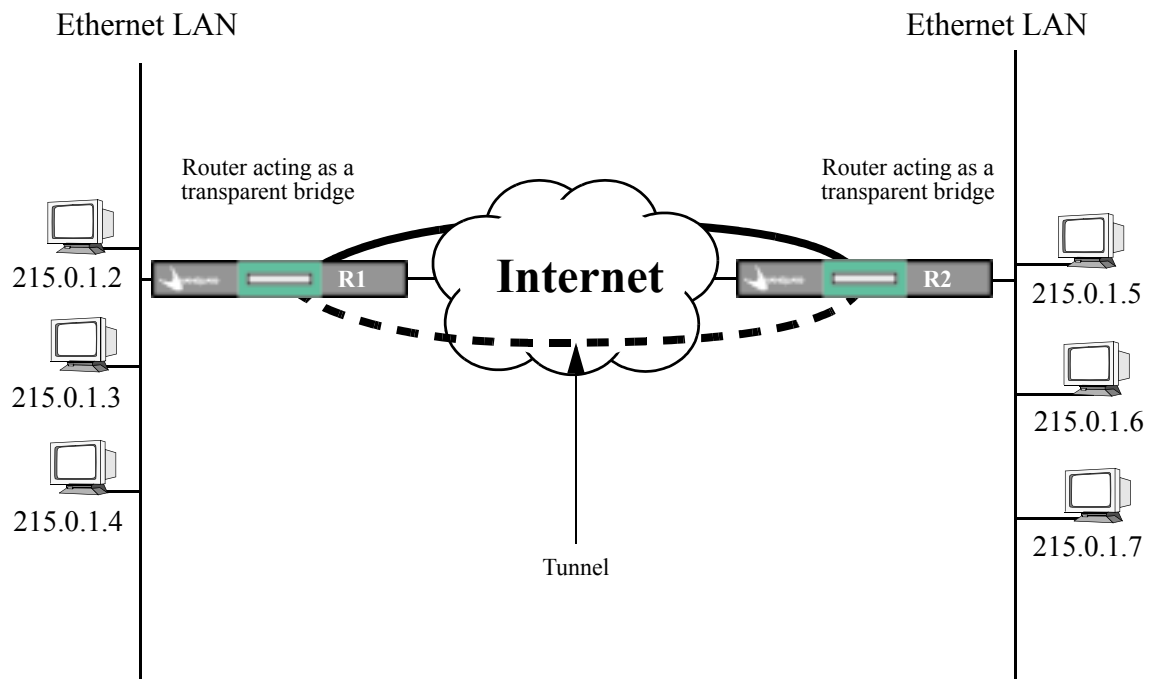
Figure 1-6 shows how to connect two half bridges using a tunnel. Bridge packets are transported from one LAN to the other through tunneling. The type of LANs used at the remote ends can be the same or different.

The overall configuration guidelines of tunnel support for bridge traffic are:

- Configure each tunnel with a unique Bridge Link Number. The Bridge Link can be Transparent, Source Routing or Translational Bridge Traffic.
- All bridge packets intended for the remote side bridge, passing through the tunnel are encapsulated with encrypted GRE and IP headers, and then sent over the tunnel.
- On the remote side tunnel, the IP and GRE Headers are removed after decryption and the original bridge packet is forwarded to the appropriate host.
- Source Routing Bridge, Transparent Bridge, and Translational Bridge traffics can be tunneled.
- For SR Bridge Traffic over a LAN Tunnel, the “Link Mode” must be configured as RFC1294 in the Bridge Link Configuration, corresponding to the Tunnel.

### ■ Note

For more information on configuring your Vanguard device for tunneling, refer to the “Tunnel Configuration” section in Chapter 2.

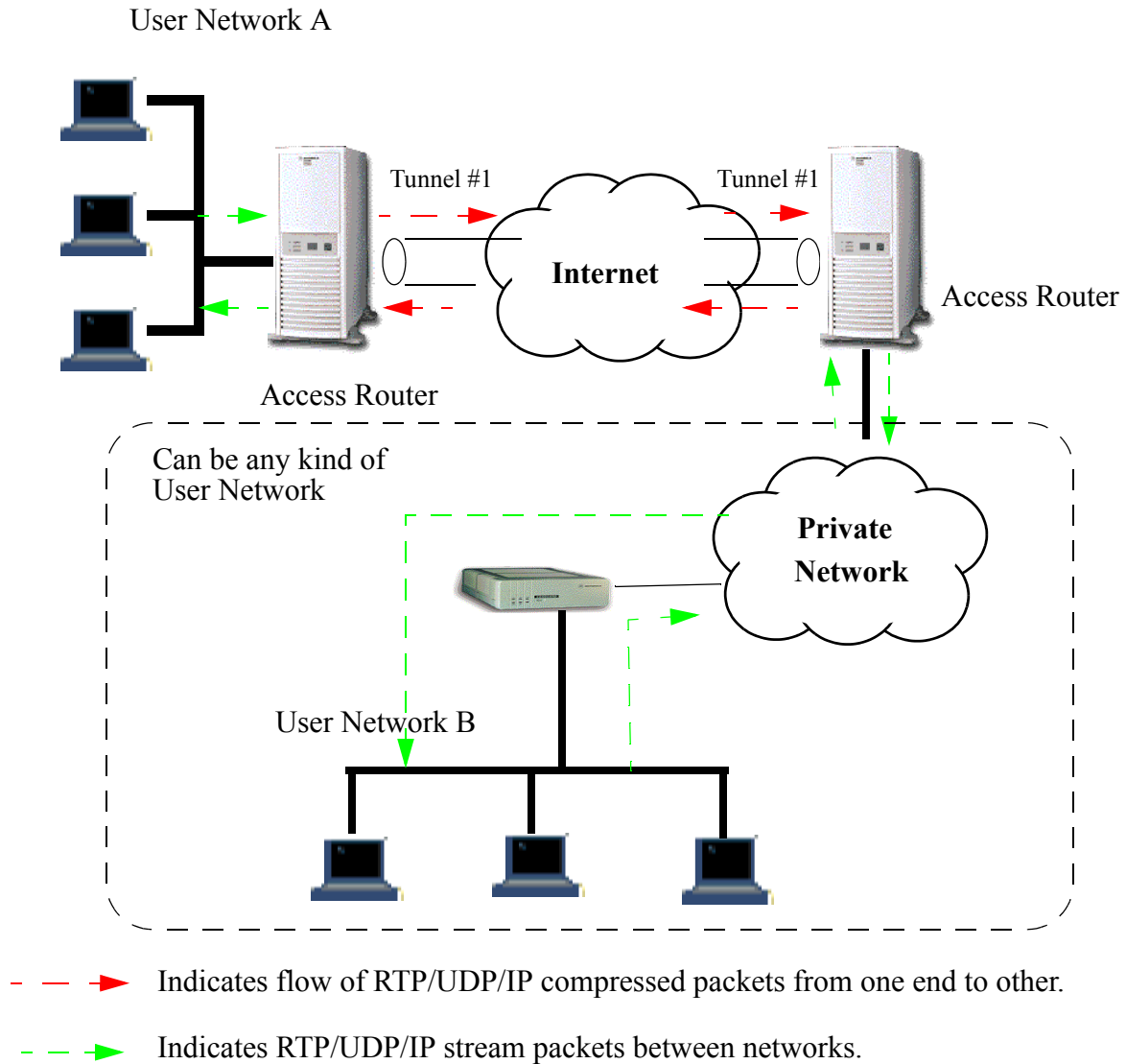


**Figure 1-6. Bridged Packets Transported Using a Tunnel**

For more information on configuring a bridge for your Vanguard device, refer to the Bridging Manual (Part number T0100-02).

**RTP/UDP/IP  
compression of  
tunneled packets**

Figure 1-7 shows an example of RTP/UDP/IP header compression between user network A and user network B. If there is a RTP stream transmitted over the tunnel (tunnel #1), RTP/UDP/IP header compression feature can be enabled to save the bandwidth usage.



**Figure 1-7. RTP/UDP/IP Header Compression**

### Overview

#### Introduction

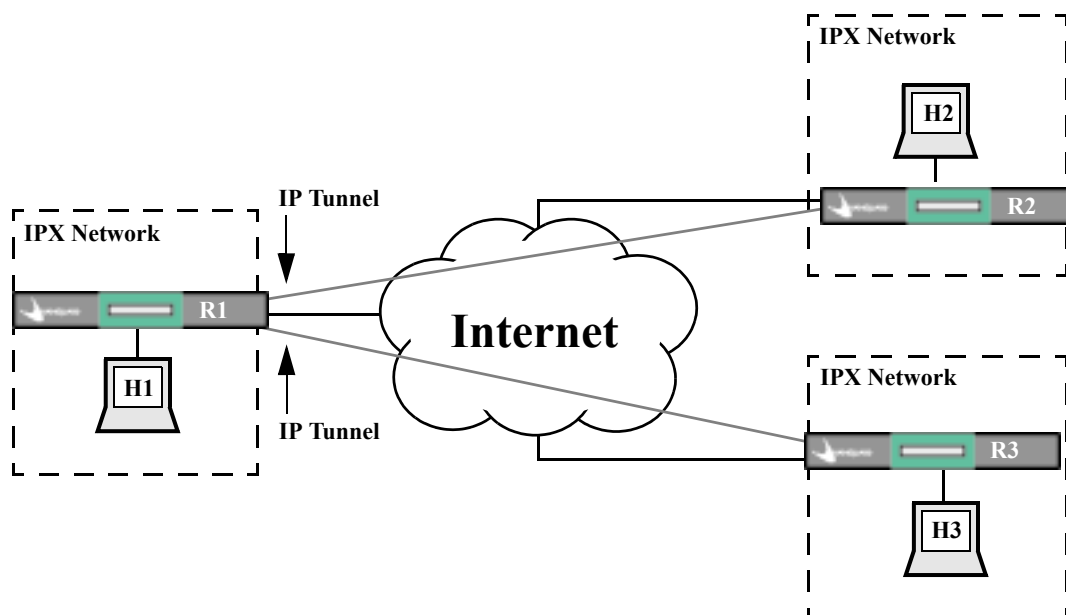
This chapter provides a detailed description of tunneling and Generic Routing Encapsulation (GRE) with respect to Vanguard Networks router implementation. Tunneling and GRE configuration is included.

#### ■ Note

There are different tunneling protocols developed which are suited to specific customer needs. GRE and L2TP are the more prevalent tunneling protocols in use. The current phase of Vanguard VPN solution implements only the GRE protocol. Therefore, in the continuing sections unless otherwise mentioned, the tunneling protocol refers to GRE.

#### What is Tunneling

To understand the process of tunneling, consider connecting three IPX networks H1, H2, and H3, with a non-IPX network, such as, the Internet. It is not possible for H1 to communicate with H2 or H3, as they are separated by a non-IPX network. This problem can be solved by tunneling IPX through a carrier protocol, such as IP. Tunneling encapsulates an IPX packet inside an IP packet, which is then sent across the Internet to the destination. At the end-point, the IPX packet is decapsulated and routed to the destination IPX host. Figure 2-1.



**Figure 2-1. Tunneling**

In addition, you can establish multiple tunnels to multiple destinations using a single physical connection to the Internet. In this example, Router 1 has tunnels to both Router 2 and Router 3 over a single connection. This can be contrasted against having two separate dedicated links between Router 1 and Router 2 and Router 1 and Router 3 which involves higher cost.

**■ Note**

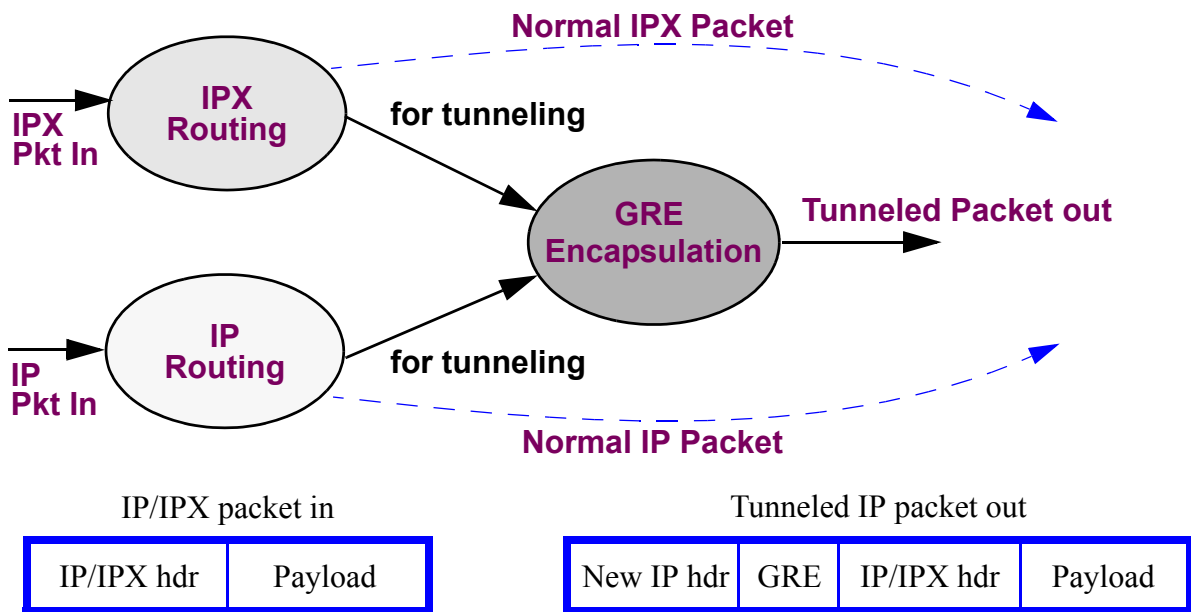
In this document, tunneling refers to forwarding multiprotocol traffic from one network to another network through IP. However, realistically, any other network *traffic* can be tunneled over any other network *protocol*.

**The Tunneling Operation (Outbound)**

Before a packet leaves the router, the router checks the tunneling configuration. If the router is configured for tunneling, the packet is forwarded for GRE (Generic Routing Encapsulation). Once the GRE is done, a new IP header containing the GRE protocol (in the protocol field) is added to the packet, and the packet is then sent out of the node. Figure 2-2 shows outbound tunneling.

**■ Note**

The tunneled packet contains the new IP header, the GRE header, and the original datagram.

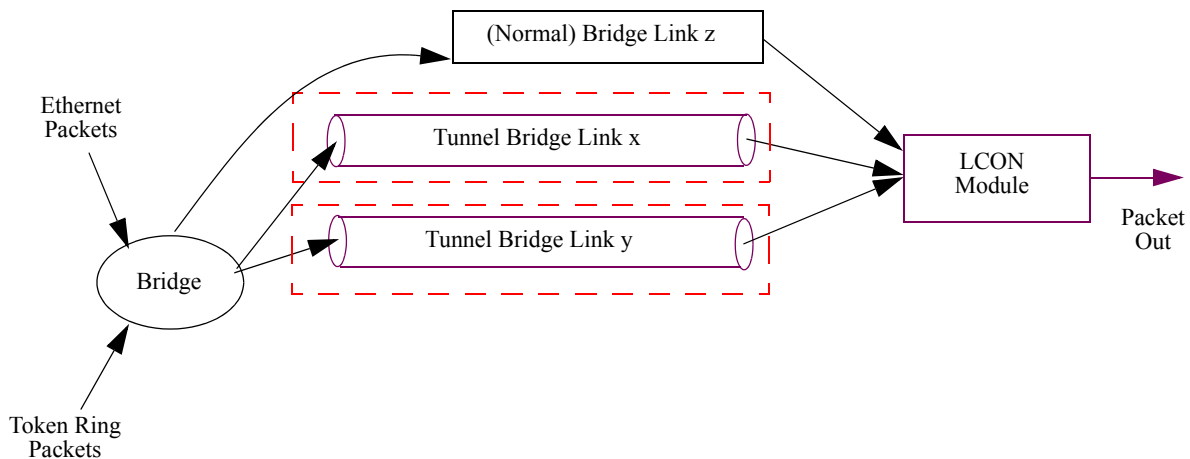


**Figure 2-2. Tunneling Operation (Outbound)**

## Tunnel Support for Bridge Traffic

Figure 2-3 shows an example of packet flow between the bridge, tunnel, and LCON modules. The overall configuration guidelines of tunnel support for bridge traffic are:

- Configure each tunnel with a unique Bridge Link Number. The Bridge Link can be Transparent, Source Routing or Translational Bridge Traffic.
- All bridge packets intended for the remote side bridge, passing through the tunnel are encapsulated with encrypted GRE and IP headers, and then sent over the tunnel.
- On the remote side tunnel, the IP and GRE Headers are removed after decryption and the original bridge packet is forwarded to the appropriate host.
- Source Routing Bridge, Transparent Bridge, and Translational Bridge traffics can be tunneled.
- The Protocol Type field in GRE Header has separate identifiers for:
  - Source Routing Bridge Packet
  - Spanning Tree Protocol Entity packet
  - Transparent Bridge packet (protocol type value = 6558)
- Tunnels support the transport of BPDU between the remote bridges for spanning tree calculations.
- For SR Bridge Traffic over a LAN Tunnel, the “Link Mode” must be configured as RFC1294 in the Bridge Link Configuration, corresponding to the Tunnel.



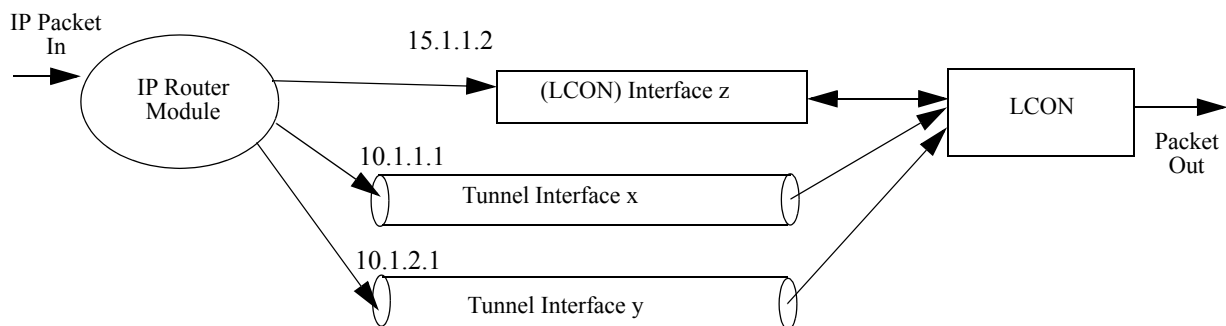
**Figure 2-3. Packet Flow between Bridge, Tunnel, and LCON Modules**

## Vanguard VPN Tunneling

**Tunnel Addresses** Each tunnel is configured with two addresses, namely, the tunnel interface address (configured in IP interface entry) and the tunnel source address (configured in Tunnel entry). The Tunnel interface addresses are only used for internal routing purposes so that the router module can forward a packet into a tunnel. The tunnel source address is put into the packet so it can be routed in the public domain. In most cases, the tunnel source address is configured as the LCON interface address.

In the following figure, three interfaces are configured in the IP interface table. One of the interfaces is connected to the LCON and has the interface address 15.1.1.2. The other two interfaces are connected to tunnels. One of the tunnels has 10.1.1.1 as the address and the other 10.1.2.1. The user has configured a static entry having the destination address X and next hop address 10.1.1.1. This indicates that any packet having the destination address X should be sent to the first tunnel. The tunnel that connects to the 10.1.1.1 interface is configured with the source address 15.1.1.2 and destination address Y.

When a packet reaches with destination address X, the router module forwards the packet to the tunnel interface x. Tunnel interface x in turn adds the GRE header and a new IP header and forwards it to the connected LCON. The new IP header has the source address as 15.1.1.2 and destination address as Y. The original destination address (which was X) and the original source address are not changed. They remain in the original IP packet header, which is placed after the GRE header. See Figure 2-4.



**Figure 2-4. Tunnel Addresses**

# Processing

## Inbound Processing

When packets enter through either an Ethernet 802.3 or Token Ring link 802.5, they are sent to the tunnel for decapsulation if there is a matching entry found in the tunnel configuration. Once the tunnel pay load is extracted after decapsulation (based on the pay load type) they are sent to either the IPX router, IP router, or Bridge. Non-tunneled packets are sent directly to the IP module. Figure 2-5 shows an example of this operation.

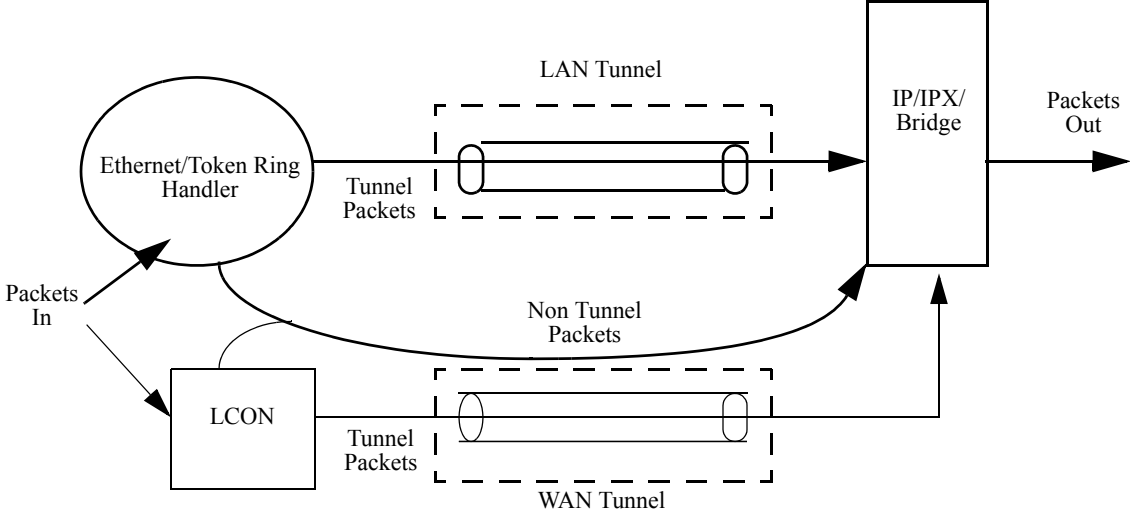
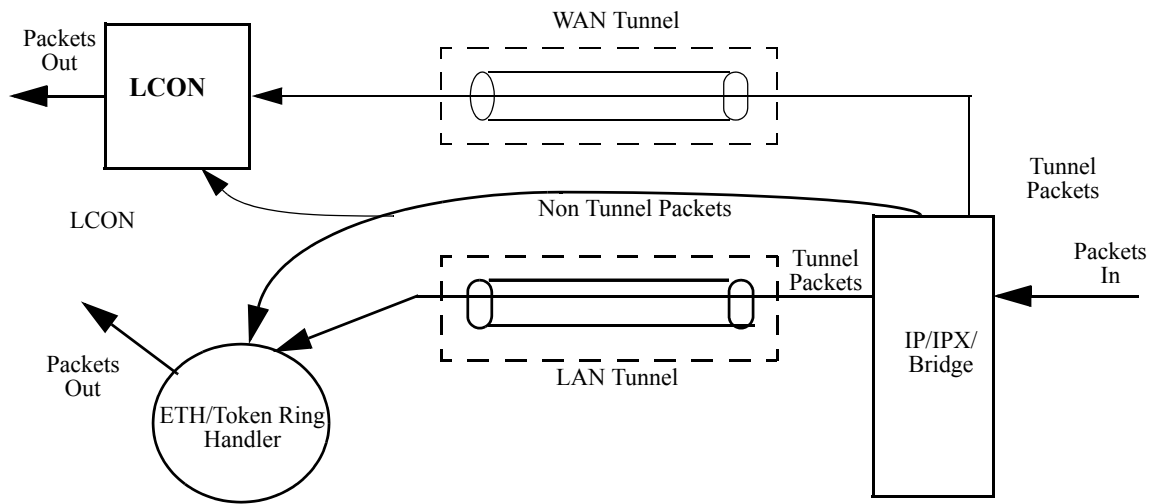


Figure 2-5. Inbound Packet Flow When a Tunnel is Terminated on a LAN

**Outbound Processing**

For LAN tunnels, IP/IPX/Bridge packets reach the tunnel module if there is a matching tunnel configured in the tunnel configuration. Packets (payload) are encapsulated with a new IP header with source and destination address configured in the matching tunnel entry. Packets are sent out on the LAN link, if a LAN tunnel is configured or a WAN link if a WAN tunnel is configured. Figure 2-6 shows an example:



**Figure 2-6. Outbound Packet Flow When a Tunnel is Over a LAN**

**Multiple Tunnels over a Single LCON**

A user can configure multiple tunnels on a single LCON. The user configures each tunnel with a different destination address and configures all of the tunnels with the same LCON.

**Multiple Tunnels to the Same Destination over a Single LCON**

A user might need to support multiple tunnels between two end-points. This is useful if the user needs to enable encryption on one tunnel and disable encryption on another tunnel. Multiple tunnels can be configured by inputting different source addresses for each of the tunnels.

**Encryption on Tunnels**

Encryption can be either enabled or disabled for all traffic going through the tunnel. Vanguard products currently provide tunnel mode encryption.

---

<b>Traffic Types</b>	<p>Vanguard Networks Routers support tunneling for following traffic types:</p> <ul style="list-style-type: none"><li>• IP</li><li>• IPX</li><li>• Routing protocols: RIP-v1, RIP-v2, OSPF and BGP</li><li>• Broadcast packets such as local, directed and all subnet broadcasts</li><li>• Bridge</li></ul>
<b>Fragmentation and Reassembly</b>	<p>Fragmentation and Reassembly of the packet is done by the tunnel. If the packet size after adding the GRE header and Encryption header (if configured) exceeds the link's MTU, then IP level fragmentation is done by the tunnel.</p> <p>On the remote side, when a fragmented packet is received by the tunnel, it waits for all the fragments before performing other tunnel operations like GRE header removal and Decryption.</p>
<b>Network Address Translation (NAT)</b>	<p>NAT static, external address can be used as a tunnel source address. NAT does not work on a tunnel/virtual interface. Do not configure tunnel/virtual interface as NAT internal or external interfaces. If Network Address Translation (NAT) is enabled and the LCON interface is external, then the tunnel source address should be configured as one of the external addresses configured for that LCON interface.</p>
<b>Tunnel Source Address</b>	<p>The tunnel source address should be configured by the user. It is usually one of the numbered LCON physical interface addresses.</p>
<b>Access Control</b>	<p>Vanguard Networks routers do not support access control for tunneled packets. On the sending side, access control (if enabled) is performed before tunneling. On the receiving end, the tunnel is identified first (decapsulate tunnel header) and then access control is applied on the decapsulated packet.</p>
<b>Policy Based Routing</b>	<p>Policy Based Routing, along with tunneling, achieves flow based tunneling. In the Policy Based Routing configuration, you can choose the next hop address as the tunnel's interface address. When a packet matches the flow, it is forwarded to the corresponding tunnel.</p>
<b>Quality of Service</b>	<p>Currently, Quality of Service (QoS) can be configured on LCONs. QoS cannot be configured on individual tunnels. The policy of the connected LCON is applied to the tunnel packets that travel over that LCON. Since QoS is not supported for LAN links/interfaces, QoS is not supported for LAN tunnels.</p>
<b>Grouped LCON</b>	<p>The tunnel does not make any distinction between a Grouped or Point-to-Point LCON. Since only one LCON can be configured per tunnel, the tunnel simply forwards the packet to the configured LCON which can either be Grouped or Point-to-Point.</p>

---

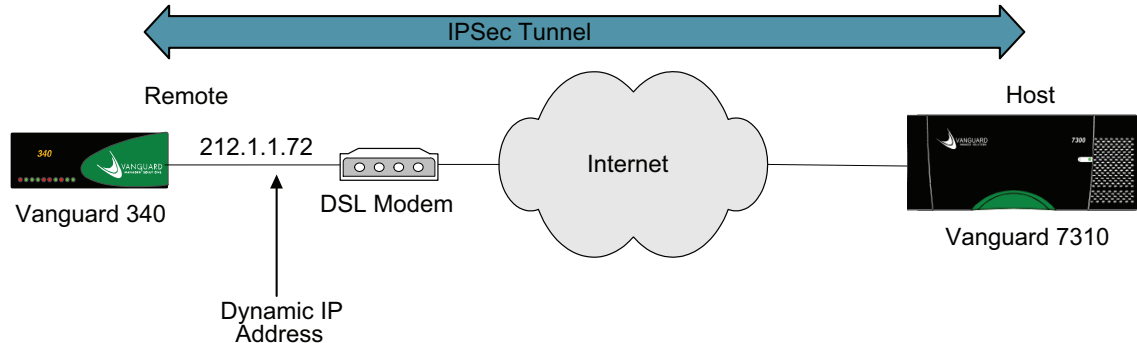
## Dynamic Tunnel Address

### Introduction

This section provides a detailed description of the Dynamic Tunnel Address feature with respect to IP Security: IPSec.

### Overview

More customers are using broadband links such as a DSL and Cable to network all their business sites. Most of the broadband service providers issue IP address dynamically to their clients, using the IP Control Protocol (IPCP) for the Point-to-Point Protocol (PPP)/ the Point-to-Point Protocol over Ethernet (PPPoE) or the Dynamic Host Configuration Protocol (DHCP). As a result, customers who secure their connections with VPN tunnels require the ability to establish IPSec tunnels over these links. The existing Vanguard VPN tunnel architecture is based on the use of static addresses to identify the tunnel endpoints. Consequently, the implementation will not work in broadband environments. The dynamic tunnel address feature aims to address the problem of establishing IPSec tunnels over links where the addresses maybe assigned dynamically. Figure 2-7 illustrates a sample scenario of a VPN tunnel with the remote side using a dynamic address.



**Figure 2-7. Tunnel Application Sample**

In this scenario,

- The remote side of the tunnel (Vanguard 340) will be able to learn the dynamic address from the DSL service provider and use it to initiate an IPSec tunnel to the host (Vanguard 7310).
- The host will be able to accept connection from a remote tunnel for which the address is not known or may change over time.

#### ■ Note

This section will describe the functionality on both the remote and host nodes. Unless otherwise noted, all further references to the remote and host sides will be in the context of Figure 2-7 unless they are not specify references. The remote side will refer to the node using the dynamic address and the host will refer the node using a static address.

## How does Dynamic Tunnel Address work?

### Remote Node

Tunnels on nodes where the IP address is provided by a server or peer will be able to learn the IP address with IPCP of PPP/PPPoE or DHCP. Once the address has been learned on the link, the address will be installed in the tunnel and the IPsec negotiations will begin and continue similarly to when using static tunnel addresses.

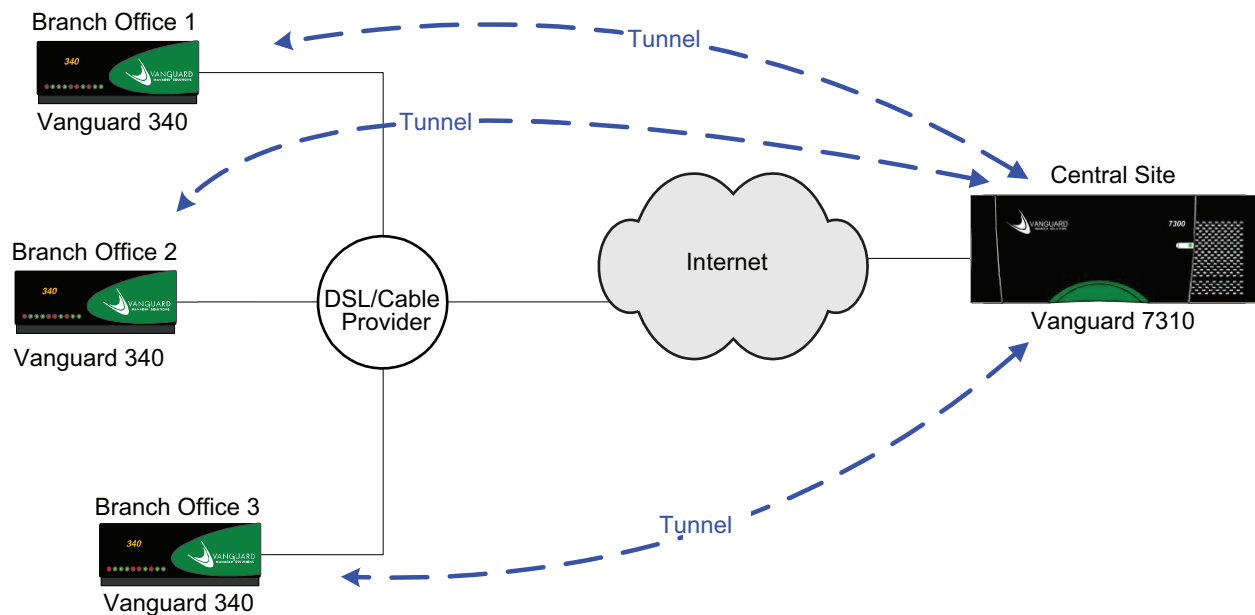
### Host Node

Currently when an incoming Internet Security Association and Key Management Protocol (ISAKMP) negotiation request is received, the ISAKMP module will identify which tunnel is for by using the source and destination address of the packet. In the dynamic address scenario, the host side is not aware of the end point address. Therefore, it will be unable to determine which tunnel the ISAKMP requests are for. The solution is to match based on ISAKMP negotiation parameters rather than the physical IP addresses. When an ISAKMP request is received, all the dynamic tunnels are examined to see whether they have any matching ISAKMP proposals. If there is a match, then that tunnel will be used to continue negotiations, comparing the pre-shared key.

To distinguish the proposals and the pre-shared keys on the tunnels, the ISAKMP policies on all the dynamic tunnels will have to be the same. In other words, the IPsec profile applied to all the tunnels with dynamic destination addresses will need to use the same IPsec profile.

#### ■ Note

Currently, the tunnels will try to establish as soon as there is connectivity to the peer. However, in the dynamic address scenario, the host side will not try to establish a tunnel connection as the remote address is not known. Instead, it will only listen for incoming tunnel negotiation requests.



**Figure 2-8. Dynamic Tunnel Address via a DSL provider**

---

### Supported Platforms

The Dynamic Tunnel Address feature will be supported on all existing platforms which support IPsec. For further information on IPsec, refer to Chapter 3, *IP Security*.

---

### Limitations

This section explains the limitations on the Dynamic Tunnel Address feature.

- All dynamic tunnels on the host will have to use the same IPsec profile. Only one profile can be used to address the different policy schemes on various remote sites using dynamic addresses.
- All pre-shared keys used on the host for remotes with dynamic addresses will have to be the same.
- In the scenario where Vanguard is the host node and the remote nodes are Cisco, and the host wants to send data to the remote, it will not be able to do so as it can not initiate a tunnel request. Cisco remotes will only negotiate a tunnel if it has data to send. So the tunnel will only be established if the remote wants to send data. In the case where the remote nodes are Vanguard, the problem does not exist because the remote Vanguard will always try to negotiate a tunnel even if there is no data to send. So, the tunnel will always be up.
- The Dynamic Tunnel Address feature will only be supported on IPsec tunnels. SAM and GRE tunnels will continue to only work with static addresses.

## Configuration Examples

### Introduction

This section provides configuration samples for the Dynamic Tunnel Address feature.

#### ■ Note

In previous releases the proxy addresses were allowed to be blank but now the proxy address parameters must be configured for dynamic tunnels since they are used for tunnel identification purposes.

### Basic Configuration

All the following configuration samples including this basic configuration sample use the same configuration parameters for Encryption and IPsec as shown in Figure 2-9, IPsec Configuration.

<p><b>Configure Encryption Parameters</b></p> <p>Enable Encryption: Enable</p>	<p><b>Configure IPsec Transform Set Table</b></p> <p>Entry Number: 1</p> <p>AH Authentication Algorithm: MD5_HMAC</p> <p>ESP Encryption Algorithm: DES_CBC</p> <p>ESP Authentication Algorithm: NONE</p>
<p><b>Configure IPsec Profile Table</b></p> <p>Entry Number: 1</p> <p>IPsec Profile Name: ipsec</p> <p>Preshared Key Name: ipseckey</p>	<p><b>Configure Preshared Key Table</b></p> <p>Entry Number: 1</p> <p>Preshared Key Name: ipseckey</p> <p>Preshared Key Value: 123</p>
<p><b>Configure ISAKMP Policy Table</b></p> <p>Entry Number: 1</p> <p>Authentication Method: PRESHARED_KEY</p> <p>Diffie-Hellman MODP Group: 1</p> <p>Encryption Algorithm: DES_CBC</p> <p>Pseudo Random Function: MD5</p>	

**Figure 2-9. Encryption and IPsec Configuration**

#### ■ Note

The examples show critical parameters only for Dynamic Tunnel Address Operation. Use default values for IP related parameters not shown.

## Remote Node

Remote Node users will only need to configure the Source Address parameter in the Tunnel Configuration Table in order to set up IPsec tunnels with dynamic source addresses. The Tunnel Configuration Table is shown below with the sample configuration for the Source Address. Configuring a source address of 0.0.0.0 will allow the source address to be learned from the WAN or LAN link that the tunnel is associated with.

### ■Note

The destination address on Remote Node has to be static: it has to be Host Node's Source Address.

### Configure Tunnel Table

```
Entry Number: 1/  
[1] Security Protocol: IPSEC/  
[1] Tunnel Source Address: 0.0.0.0/  
[1] Tunnel Destination Address: 212.1.1.72/  
[1] Tunnel Source Proxy Address: 192.168.1.0/  
[1] Tunnel Source Proxy Mask: 255.255.255.0/  
[1] Tunnel Destination Proxy Address: 192.168.2.0 /  
[1] Tunnel Destination Proxy Mask: 255.255.255.0/  
[1] Lcon No: 0/  
[1] LAN nexthop IP Address: 212.1.1.1/  
[1] Tunnel Interface No: 5/  
[1] Encryption Profile: ipsec/  
[1] Debug: Disabled/
```

## Host Node

A dynamic tunnel destination address is configured similarly to the dynamic source address. Configuring 0.0.0.0 as the destination address will create dynamic tunnel that is able to receive tunnel requests from a peer with a dynamic address. Users will have to configure a tunnel record for each remote site that will connect to the host. Once the link that the tunnel is associated with is up, the tunnel will listen for incoming requests. Upon the successful negotiation of the tunnel, it will operate similarly to a tunnel using static addresses.

### ■Note

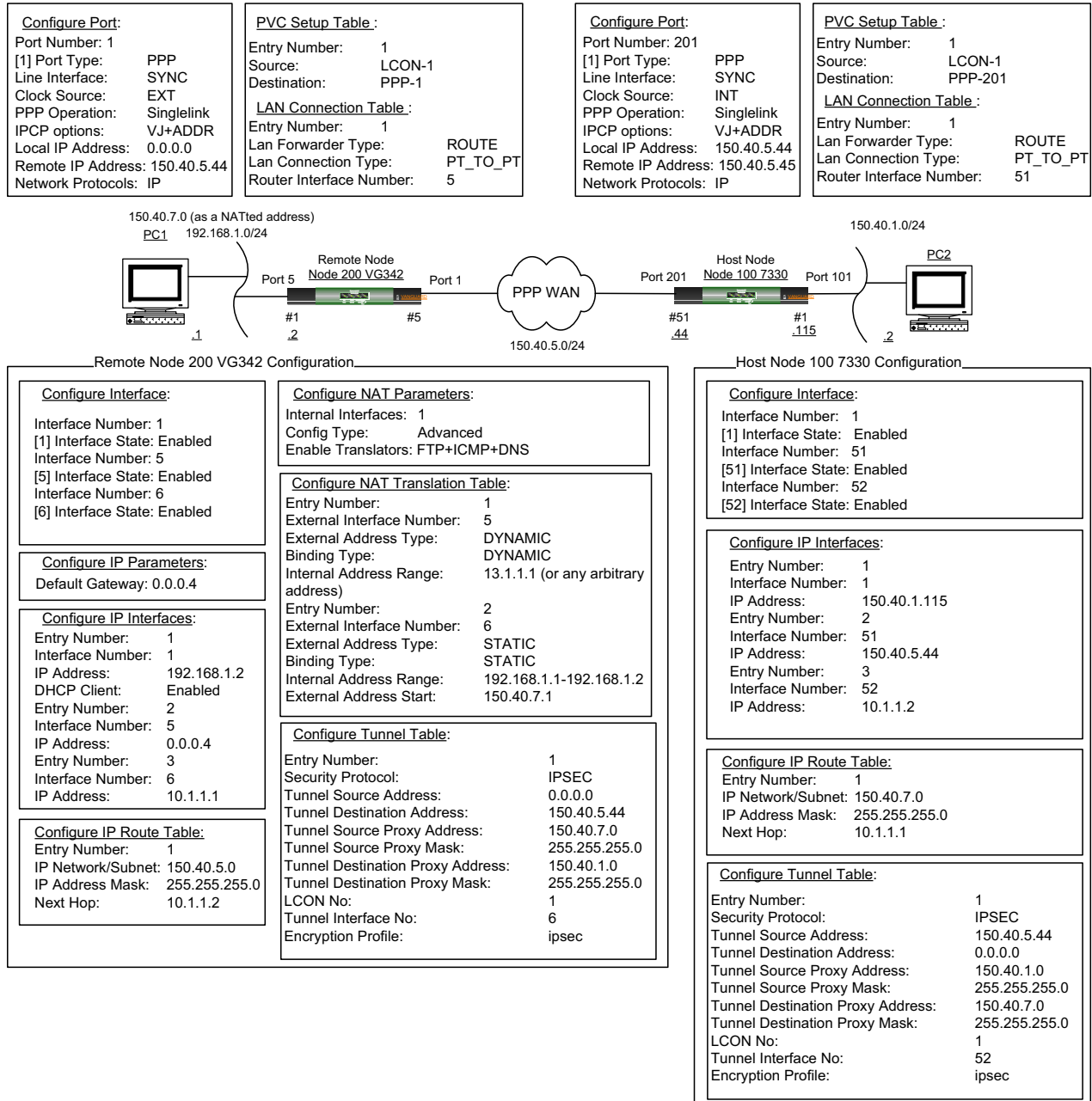
The source address on Host Node has to be static.

### Configure Tunnel Table

```
Entry Number: 1/  
[1] Security Protocol: IPSEC/  
[1] Tunnel Source Address: 212.1.1.72/  
[1] Tunnel Destination Address: 0.0.0.0/  
[1] Tunnel Source Proxy Address: 192.168.1.0/  
[1] Tunnel Source Proxy Mask: 255.255.255.0/  
[1] Tunnel Destination Proxy Address: 192.168.2.0 /  
[1] Tunnel Destination Proxy Mask: 255.255.255.0/  
[1] Lcon No: 0/  
[1] LAN nexthop IP Address: 212.1.1.1/  
[1] Tunnel Interface No: 5/  
[1] Encryption Profile: ipsecdynamic/  
[1] Debug: Disabled/
```

**PPP Over WAN Example**

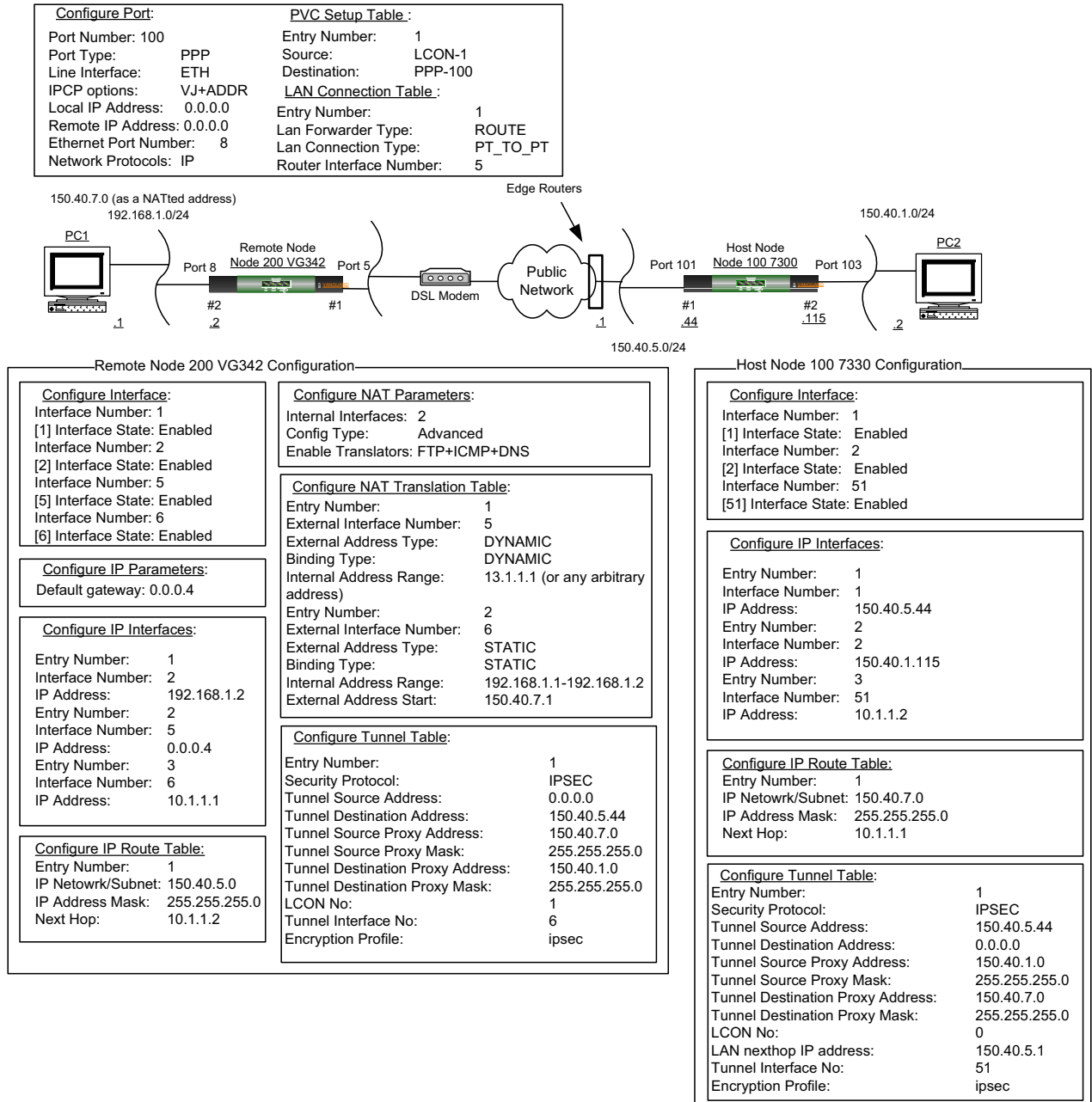
Figure 2-10 details the configuration required for using the Dynamic Tunnel Address feature via PPP over WAN.



**Figure 2-10. Dynamic Tunnel Address Example with PPP over WAN**

**PPP over Ethernet Example**

Figure 2-11 details the configuration required for using the Dynamic Tunnel Address feature via PPP over Ethernet.



**Figure 2-11. Dynamic Tunnel Address Example with PPP over Ethernet**

## DHCP Example

Figure 2-12 details the configuration required for using the Dynamic Tunnel Address feature via DHCP.

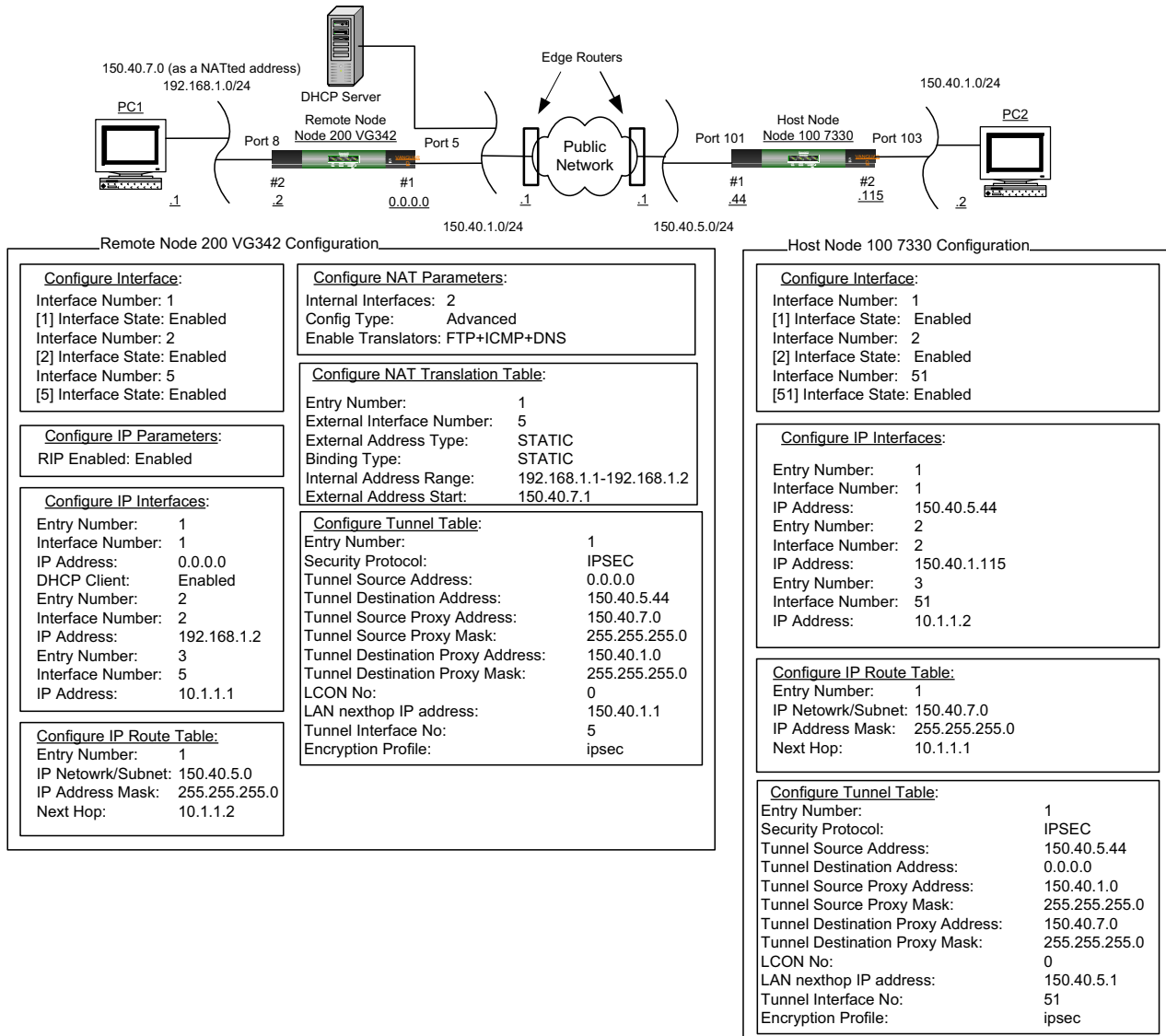


Figure 2-12. Dynamic Tunnel Address feature via DHCP

## Dynamic Tunnel Address Statistics

### Introduction

This section describes the tunnel statistics of node with a tunnel with the Dynamic Tunnel Address feature.

### Examining General Tunnel Statistics

Use these steps to examine general tunnel statistics:

Step	Action	Result
1	Select <b>Status/Statistics</b> , from the CTP Main menu.	The Status/Statistics menu appears.
2	Select <b>Router Stats</b> .	The Router Stats menu is displayed.
3	Select <b>Tunnel Statistics</b> .	The Tunnel Statistics menu is displayed.
4	Select <b>General Tunnel Statistics</b> .	A screen similar to the one in Figure 2-13 is displayed.

```

Node: Address:                               Date:                               Time
Tunnel Statistics

Tnl  Tunnel          Tunnel          Prot Packets  Packets  Packets  Encr  RUIHC
No.  Source           Destination     Sent   Rcvd    Dropped Stat  Stat
-----
  1  217.1.84.28      219.1.85.2     IP    120    89      2    NA  DIS
  2  217.1.84.34      219.1.85.2     IP     56    78      7   DATA DIS
  3  217.1.84.34      219.1.85.2     IPX    68    90     10   DATA DIS
  4  217.1.84.34      219.1.86.4     BRID   12   100     2   DATA DIS
    
```

**Figure 2-13. Tunnel Statistics Screen**

For further information on the General Tunnel Statistics Screen terms, refer to Chapter 2, *Tunneling*, in the *Virtual Private Network (VPN)* manual.

**Statistics on Remote Node**

Figure 2-14 illustrates the tunnel statistics of node with a tunnel with a dynamic source address. This occurs before the tunnel has learned the dynamic address.

```

Node: v342-1      Address: (blank)      Date: 4-JUN-2004  Time: 13:25:17
Tunnel Statistics

Tnl  Tunnel      Tunnel      Prot  Packets  Packets  Packets  Encr  RUIHC
No.  Source      Destination Sent  Received Dropped Stat  Stat
-----
  3  0.0.0.0      192.168.1.29  IP      0         0         0  IDLE  DIS

Press any key to continue ( ESC to exit ) ...
    
```

**Figure 2-14. Tunnel Statistics of Node with a Tunnel with a Dynamic Source Address.**

Once the address is learned, the address will be visible in the statistics screen. An asterisk (\*) will be appended to tunnel source addresses which are learnt.

```

Node: v342-1      Address: (blank)      Date: 4-JUN-2004  Time: 13:25:17
Tunnel Statistics

Tnl  Tunnel      Tunnel      Prot  Packets  Packets  Packets  Encr  RUIHC
No.  Source      Destination Sent  Received Dropped Stat  Stat
-----
  3  192.168.1.3*  192.168.1.29  IP      0         0         0  IDLE  DIS

Press any key to continue ( ESC to exit ) ...
    
```

**Figure 2-15. Address on the Statistics Screen**

**Statistics on Host Node**

Similar to the remote node, the tunnel statistics of a host node with a tunnel to a dynamic remote is shown in Figure 2-16. It shows an idle tunnel awaiting a request from the remote node.

```
Node: v342-1      Address: (blank)      Date: 4-JUN-2004  Time: 13:25:17
Tunnel Statistics

Tnl  Tunnel      Tunnel      Prot  Packets  Packets  Packets  Encr  RUIHC
No.  Source      Destination  -----  -----  -----  -----  -----
-----  -----  -----  -----  -----  -----  -----  -----
  3   219.1.245.1  0.0.0.0      IP      0         0         0         0  IDLE  DIS
```

Press any key to continue ( ESC to exit ) ...

**Figure 2-16. Tunnel Statistics of Host Node with a Tunnel to a Dynamic Remote**

Upon the successful negotiation of the tunnel, the remote address will be shown. An asterisk (\*) will be appended to tunnel destination addresses of tunnels for which the remote is dynamic.

```
Node: v342-1      Address: (blank)      Date: 4-JUN-2004  Time: 13:25:17
Tunnel Statistics

Tnl  Tunnel      Tunnel      Prot  Packets  Packets  Packets  Encr  RUIHC
No.  Source      Destination  -----  -----  -----  -----  -----
-----  -----  -----  -----  -----  -----  -----  -----
  3   219.1.245.1  219.1.245.19*  IP      0         0         0         0  IDLE  DIS
```

Press any key to continue ( ESC to exit ) ...

**Figure 2-17. Tunnel Destination Addresses of Tunnels for which the Remote is Dynamic**

## RTP/UDP/IP Header Compression of Tunneled Packets

---

**Introduction** This section provides a detailed description of the RTP/UDP/IP Header Compression of tunnel packets with respect to Vanguard routers.

---

**How does it work?** RTP/UDP/IP Header Compression of tunnel packets is designed to reduce the RTP/UDP/IP or UDP/IP (Voice Payload) header. In cases where no UDP checksum is sent, the header is reduced to two bytes for most of the packets. When checksums are sent, the header is reduced to four bytes. This provides a mechanism for efficient bandwidth usage where link cost is relatively high or the packet has to be transferred over a low-speed link.

---

**RTP/UDP/IP Header Compression Process** When using RTP/UDP/IP Header Compression over a tunnel, once the RTP/UDP/IP stream has been identified for compression, the RTP/UDP/IP header is compressed from 40 bytes to either 2 or 4 bytes. This compressed packet is encapsulated with a GRE and IP header, and then sent over the tunnel.

The overall characteristics of RTP/UDP/IP Header Compression of tunnel packets are:

- RTP/UDP/IP compression profile must be configured per tunnel.
- When RTP/UDP/IP Header Compression is enabled across a tunnel, there are compressor and decompressor modules residing on each edge of the tunnel.
- If the incoming payload packet to the tunnel is an IP packet, it is given to the RTP/UDP/IP header compression module that detects a RTP flow, compresses the RTP/UDP/IP header, and gives back the compressed packet to the tunnel.
- Compressed packet is encapsulated with a GRE and IP header, and then sent over the tunnel.
- On the receiving side, if the compression module exists, the compressed packet is given to decompression module.
- The decompressor identifies the flow, decompresses the packet and sends it back to the tunnel.
- For SR Bridge Traffic over a LAN Tunnel, the “Link Mode” must be configured as RFC1294 in the Bridge Link Configuration, corresponding to the Tunnel.

For more information on configuring your Vanguard device, refer to the “Configuration Examples” section on page 2-32.

---

## Generic Routing Encapsulation (GRE)

**Introduction** This section provides a detailed description of the GRE protocol with respect to Vanguard Networks' Vanguard routers.

**What is GRE** GRE is a protocol which encapsulates multiprotocol data and sends the encapsulated packet through bidirectional IP tunnels that exist between source and remote routers. GRE is identified by protocol number 47. GRE is discussed in RFC 1701.

**GRE Protocol Header** Figure 2-18 shows the GRE protocol header.

0	1	2	3	4	5 - 7	8 - 12	13 - 15	16 - 31
<b>C</b>	<b>R</b>	<b>K</b>	<b>S</b>	<b>s</b>	<b>Recur</b>	<b>Flags</b>	<b>Ver</b>	<b>Protocol Type</b>
<b>Checksum (Optional)</b>							<b>Offset (Optional)</b>	
<b>Key (Optional)</b>								
<b>Sequence Number (Optional)</b>								
<b>Routing (Optional)</b>								

**Figure 2-18. GRE Protocol Header**

**GRE Header Bits** This table describes the elements contained in a GRE protocol header.

<b>Bit Number</b>	<b>Function</b>
Checksum Present (bit 0)	If this bit is set, the checksum field is present and contains valid information.
Routing Present (bit 1)	This field is currently not being used.
Key Present (bit 2)	This field is currently not being used.
Sequence Number (bit 3)	If this bit is set, it indicates that sequence number is present in the GRE header. This sequence number is set by the transmitter. At the remote end, the receiver checks if the current packet's sequence number is greater than (if the size is N then check $> N/2 - 1$ ) the previous packet's sequence number. If it is then it allows the packet to pass. If not, it drops the packet. This field is currently not being used and is set to zero.

<b>Bit Number</b>	<b>Function (continued)</b>
Strict Source Route (bit 4)	This field is not being used.
Recursion Control (Bit 5 - 7)	This field is defaulted to zero.
Version Number (bit 13 - 15)	The version number field is set to zero.
Protocol Type (Bit 16 - 31)	This field contains the protocol type of the payload packet. e.g. IP = 0800h, Raw Frame Relay = 6559h, Novel IPX = 8137h.
Checksum (2 Octets)	This field contains the IP checksum of the GRE header and payload packet. It contains valid information only if the Checksum Present bit is set to 1.
Offset (2 Octet)	This field contains the octet offset from the start of the Routing field to the first octet of the active source route entry. It contains valid information only if the Routing Present bit is set to 1.
Key (4 Octets)	Not Applicable.
Sequence Number (4 Octets)	This field contains an unsigned 32 bit integer value and it is used by the receiver to establish the order in which packets are transmitted from encapsulation to the receiver. Currently, this field is not being used.
Routing (Variable)	This field is optional and is present only if the Routing Present bit is set to 1.

**New IP Header**

This table describes the fields present in the new IP header added by the tunnel.

<b>Field</b>	<b>Function</b>
Source Address	Refer to Tunnel Addresses page 1-4.
Destination Address	This field contains the tunnel destination address configured by the user.
Fragment Offset	If the packet size is greater than the MTU size then packet needs to be fragmented. This field specifies the offset in the original datagram of the data being carried in the fragment.
Flags and Identification	The first two bits in the Flag and Identification field control the fragmentation and is copied from the original datagram.
Protocol	This field contains the value 47 which means that the data portion of the datagram contains GRE protocol.
TTL	This field contains a default value of 60.
Checksum	This field contains the checksum for the new IP header.
Options	This field is not used.
	The remaining fields are copied from the original IP datagram.

---

**Sequence Number  
Support to GRE  
Header**

To ensure that GRE Payload packets arrive at their destination in-order, sequence numbers can be assigned to the GRE packets. When configuring your Vanguard device for GRE, include SEQ to display the *GRE Resynchronization Counter* parameter. This parameter lets you determine the number of out-of-order packets to be discarded before resynchronizing with the sender's sequence number.

For more information on configuring your Vanguard device, refer to the "Configuration Examples" section on page 2-32.

---

## Next Hop Resolution Protocol (NHRP)

---

<b>Introduction</b>	This section describes the NHRP Protocol with respect to the Vanguard Networks' Vanguard routers.
<b>What is NHRP</b>	The Next Hop Resolution Protocol (NHRP) allows a source station (a host or router), wishing to communicate over a Non-Broadcast, Multi-Access (NBMA) sub-network, to determine the internetworking layer addresses and NBMA addresses of suitable "NBMA next hops" toward a destination station.
<b>Vanguards NHRP</b>	<p>NHRP support is now available in the 7.3 release.</p> <p>NHRP was introduced in response to the demand for Vanguard Network routers to operate in the DMVPN (Dynamic Multipoint Virtual Private Network) model.</p> <p>In the DMVPN model NHRP was required to address the burden of the HUB router in managing its remotes, primarily in the hubs requirement to add configuration for each of the remotes in the network. Using NHRP the Hub no longer has the need to modify/add to the configuration for any remotes added to the network.</p> <p>The Vanguard Networks 7.3 release of NHRP support includes the following;</p> <ul style="list-style-type: none"><li>• Act as Spokes in the Hub &amp; Spoke network</li><li>• Use GRE to transport data to the Hub (GRE only)</li><li>• Support dynamic IP addressing on the WAN interface.</li></ul> <p>The 7.3 release of Vanguard Networks NHRP implementation does NOT require the Vanguard routers to:</p> <ul style="list-style-type: none"><li>• Act as Hubs</li><li>• Be an NHRP Server</li><li>• Support direct Spoke-to-Spoke tunnels</li><li>• Support dynamic caching of mappings.</li></ul> <p>The Spokes will always have a static NHRP mapping for the Hub. The Hub must have a static IP address that is known by the Spokes.</p>
<b>GRE Enhancements</b>	<p>In support of the NHRP implementation an optional GRE Key (Tunnel Key) is needed to provide a way for the hub routers to map incoming GRE packets to specific tunnel interfaces. Each tunnel interface on a router must have a distinct GRE Key. All tunnels in a given DMVPN must have the same key.</p>

---

# Tunnel Configuration

## Introduction

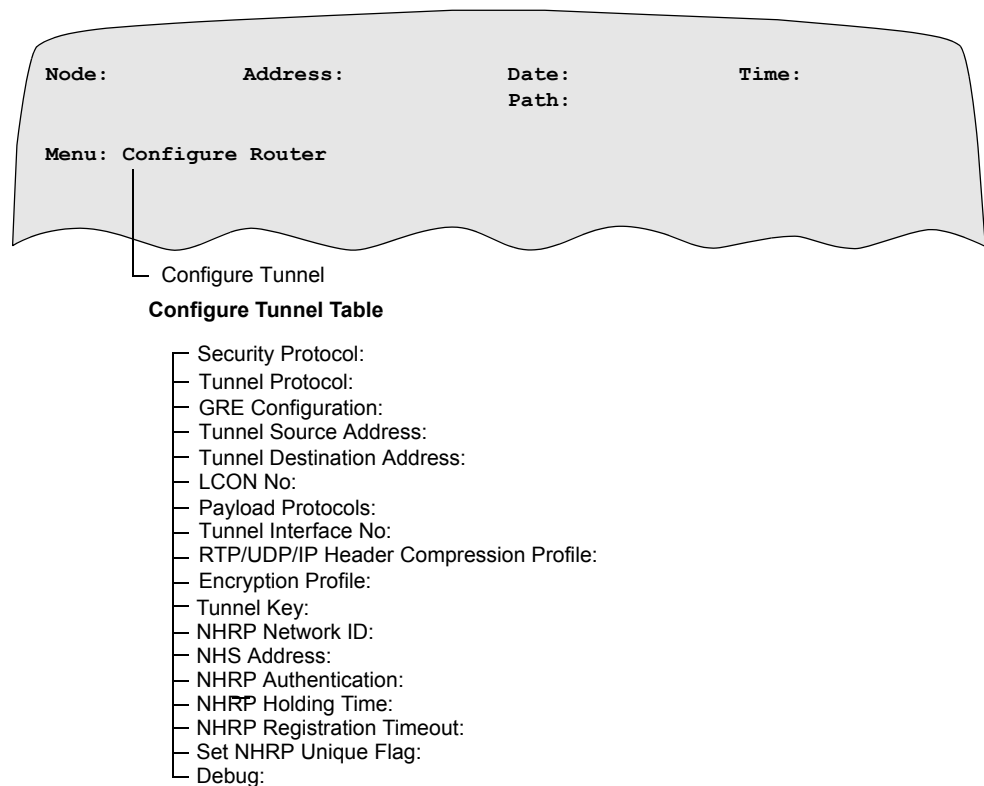
This section explains Tunnel configuration in detail.

## Tunnel Configuration Menu

To create a tunnel, you must specify various parameters in the router's configuration such as, the tunnel address, the tunnel interface number, etc. Figure 2-19 shows an example of the CTP configuration for tunneling and encryption.

**Note**

Encryption is discussed in more detail later in this document.



**Figure 2-19. Tunnel Configuration Parameters**

## Parameters

### Entry Number

Range:	1 to 255
Default:	1
Description:	Entry number used to reference this table record.

**Security Protocol: IPSEC/?**

Range:	NONE, SAM, IPSEC
Default:	NONE
Description:	<p>This parameter specifies the Security mechanism used for the tunnel.</p> <ul style="list-style-type: none"> <li>• NONE - No security mechanism should be used</li> <li>• SAM - Proprietary protocol, used for all types (IP/IPX/BRIDGE) of traffic</li> <li>• IPSEC - Generic Security protocol, this will be used only for IP traffic.</li> </ul> <p><b>■ Note</b>  For a non-encrypted tunnel, the Security Protocol should be set to NONE.  For a GRE_IPSEC tunnel, the Security Protocol should also be specified as NONE, since a second IPSEC tunnel is configured for performing the security.</p>

**Tunnel Protocol: GRE/?**

Range:	GRE, GRE_IPSEC
Default:	GRE
Description:	<p>This parameter specifies the protocol used for tunneling.</p> <p>The protocols supported are:</p> <ul style="list-style-type: none"> <li>• GRE - Generic Routing Encapsulation(GRE) should be applied on this tunnel</li> <li>• GRE_IPSEC : Generic Routing Encapsulation is first applied on this tunnel, after which the packet is passed onto a specified IPsec tunnel interface so that the IP Security features configured on that tunnel can be applied. If this option is chosen, the user must specify a valid IPsec tunnel interface (below).</li> </ul> <p>If the tunnel type is GRE_IPSEC and the security protocol is subsequently changed to IPSEC, the user MUST change the tunnel type to GRE (default).</p>
Guidelines	Appears only if Security Protocol is configured for SAM.

### GRE Configuration

Range:	NONE, CKS, SEQ, COMP
Default:	NONE
Description:	<p>This parameter specifies if GRE checksum and sequence number are enabled. It also specifies whether GRE tunnel is compatible with older nodes for sequence numbers and checksum options. A combination of these can also be specified.</p> <p>Example: CKS+SEQ+COMP</p> <p>The tunnel does not provide security or guarantee packet integrity. This can be achieved by:</p> <p>Enabling end-to-end Checksum - the router drops corrupted packets.</p> <p>Enabling Sequence Number - the router drops datagrams that arrive out of order.</p>
Guidelines	Appears only if Tunnel Protocol is configured to GRE.

### GRE Resynchronization Counter

Range:	1 to 64
Default:	8
Description:	<p>This parameter specifies the number of packets that the node can drop before it resynchronizes with the sender. When the sending node is booted, the sequencing number of the packet sent starts from the first number. Since the receiving node is expecting packets with a sequence number greater than what it has received, the packets received are dropped until the sequence number reaches the value currently held in the node.</p> <p>To synchronize the counters of both nodes, this parameter is configured so that a specific number of packets are dropped before the node sets its expected sequence number to the received sequence number.</p> <p><b>Note</b> This is a delicate parameter and should be modified only when necessary.</p>
Guidelines:	Appears only if the GRE Configuration type includes SEQ.

**Tunnel Source Address**

Range:	A valid IP Address in dotted notation.
Default:	0.0.0.0
Description:	This parameter is used to specify the source address of the tunnel. This address is put into the source address field of the tunnel packet.

**Tunnel Destination Address**

Range:	A valid IP Address in dotted notation.
Default:	0.0.0.0
Description:	This parameter is used to specify the IP address of the remote end of the tunnel in dotted decimal notation.

**Tunnel Source Proxy Address**

Range:	A valid IP Address in dotted notation.
Default:	0.0.0.0
Description:	This parameter is used to specify the source proxy address of the tunnel. This address is used when IP SEC encryption is used over the tunnel.
Guidelines:	Appears only if Security Protocol is configured for IPSEC.

**Tunnel Source Proxy Mask**

Range:	255.0.0.0 to 255.255.255.255
Default:	255.255.255.0
Description:	This parameter is used to specify the range of the source proxy address of the tunnel. This address is used when IP SEC encryption is used over the tunnel.
Guidelines:	Appears only if Security Protocol is configured for IPSEC.

**Tunnel Destination Proxy Address**

Range:	A valid IP Address in dotted notation.
Default:	0.0.0.0
Description:	This parameter is used to specify the destination proxy address of the tunnel. This address is used when IP SEC encryption is used over the tunnel.
Guidelines:	Appears only if Security Protocol is configured for IPSEC.

**Tunnel Destination Proxy Mask**

Range:	255.0.0.0 to 255.255.255.255
Default:	255.255.255.0
Description:	This parameter is used to specify the range of the destination proxy address of the tunnel. This address is used when IP SEC encryption is used over the tunnel.
Guidelines:	Appears only if Security Protocol is configured for IPSEC.

**LCON No**

Range:	0 to 2000
Default:	1
Description:	This parameter specifies the LCON that is used to forward the tunneled packets. <ul style="list-style-type: none"> <li>• 1 - 2000 For tunnels going on WAN link.</li> <li>• 0: For tunnels going on LAN link.</li> </ul>

**LAN nexthop IP Address**

Range:	A Valid IP Address in dotted notation.
Default:	0.0.0.0
Description:	This parameter specifies the nexthop IP address corresponding to a LAN interface which is used to forward the tunneled packets.
Guidelines:	Appears only if LCON No is zero.

**Payload Protocols**

Range:	IP, IPX, BRIDGE
Default:	IP
Description:	This parameter specifies the accepted protocol types of the payload data. If the packet protocol type does not match the configured protocol type then the packet is dropped. A combination of these can be specified. Example: IP+IPX+BRIDGE
Guidelines:	Appears only if Security Protocol is configured for SAM.

**Tunnel Interface No**

Range:	5 to 1000
Default:	5
Description:	This parameter specifies the router interface used by this tunnel.
Guidelines:	Appears only if Payload Protocol includes IP, IPX, or Security Protocol is configured for IPSEC.

**RTP/UTP/IP Header Compression Profile**

Range:	0 to 8 alphanumeric characters. (Use the space character to blank the field.)
Default:	(blank)
Description:	This parameter specifies the name of the RTP/UDP/IP Header Compression Profile used by this tunnel.
Guidelines:	Appears only if Payload Protocol includes IP.

**Tunnel Bridge Link No**

Range:	5 to 250
Default:	5
Description:	This parameter specifies the bridge link used by this tunnel.
Guidelines:	Appears only if Payload Protocol includes BRIDGE.

**Encryption Profile**

Range:	1 to 15 alphanumeric characters. (Use the space character to blank the field.)
Default:	(blank)
Description:	This parameter specifies the profile name of the Encryption Profile Table.

**Tunnel Key**

Range	0-4294967295
Default	0
Description	This parameter enables the use of the optional Key field in the GRE header. A value of 0 indicates the GRE Key is not used.

### NHRP Network ID

Range	0-4294967295
Default	0
Description	This is an identifier for a specific NHRP network. Each NHRP network must have a unique Network ID. All nodes in the network must have the same Network ID. A value of 0 indicates the Network ID is not used.

### NHS Address

Range	A valid IP address in dotted notation.
Default	0.0.0.0
Description	This parameter specifies the address of the Next Hop Server (NHS). The router will register with the NHS.

### NHRP Authentication

Range	0-8 alphanumeric characters, use the space character to blank field
Default	(blank)
Description	This parameter specifies the authentication string used in NHRP messages. If blank, authentication is not used.

### NHRP Holding Time

Range	0-65535
Default	7200
Description	This parameter specifies the holding time value in NHRP registration requests. The NHS will cache the registration request for the duration of the holding time value in seconds.

### NHRP Registration Timeout

Range	0-65535
Default	2400
Description	Registration requests are sent out every [this parameter] seconds. If this parameter is set to 0, then registration requests are sent out every [1/3of holding time] seconds.

**Set NHRP Unique Flag**

Range	Yes,No
Default	Yes
Description	This determines whether to set the unique flag in registration requests. If the flag is set, the hub will prevent the mapping entry from being overwritten by a registration request with the same protocol address but with a different NBMA address. It's recommended to set this parameter to Yes if the tunnel's source address is static, to No if dynamic.

**Debug**

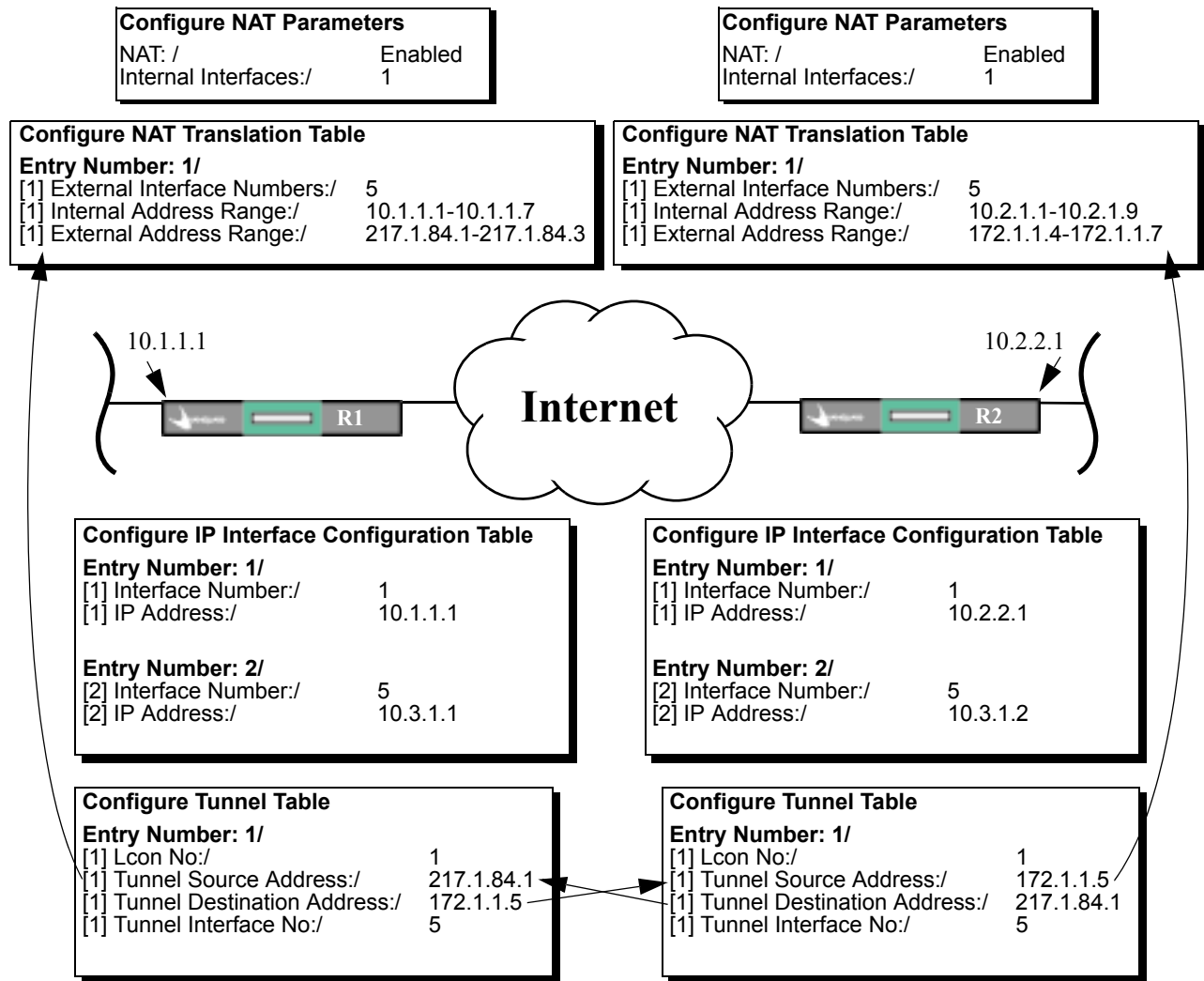
Range:	Enabled, Disabled
Default:	Disabled
Description:	This parameter enables reports for diagnostic purposes in the data passing state.

---

## Configuration Examples

### NAT and Tunnel Interoperations

Figure 2-20 details the configuration required for using NAT and tunneling techniques.



**Figure 2-20. NAT and Tunnel Interoperation**

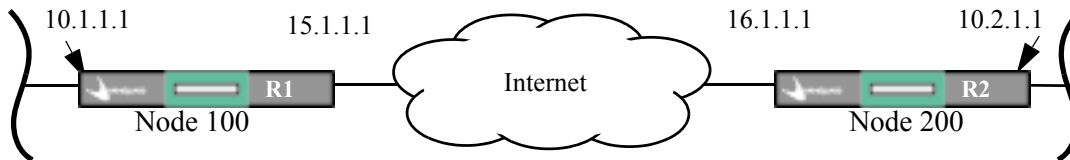
Two domains 10.1.x.x and 10.2.x.x are connected over the Internet. The Internet has assigned 3 addresses (217.1.84.1 - 217.1.84.3) to the 10.1.x.x network and 4 addresses (172.1.1.4 - 172.1.1.7) to the 10.2.x.x network. NAT is used to translate the private addresses to public address. Since tunneling is required to communicate between these two domains, the tunnel should also use a public address in its outer header so that the packets can be routed in the Internet. Hence the source addresses of the tunnels are selected from the configured NAT External Address Range (217.1.84.1 and 172.1.1.5). These addresses are bound to the router's internal address and are not available for any other host for dynamic binding.

---

**Encrypted Tunnels** Figure 2-21 shows how to configure encrypted tunnels.

## Tunnel Configuration

<b>Configure Encryption Parameters</b> *Number of Encryption Channels:/ 50 *Enable Encryption:/ enable	<b>Configure Encryption Parameters</b> *Number of Encryption Channels:/ 50 *Enable Encryption:/ enable
<b>Configure Encryption Node Key Table</b> 1st DES key: **** ***/ auto 1st DES key: C111 6B41 3894 BB** 2nd DES key: **** ***/ auto 2nd DES key: B5DE 4025 1C3B 45**	<b>Configure Encryption Node Key Table</b> 1st DES key: **** ***/ auto 1st DES key: C111 6B41 3894 BB** 2nd DES key: **** ***/ auto 2nd DES key: B5DE 4025 1C3B 45**
<b>Configure Encryption Base Key Table</b> Key Name:/ node100 1st DES key: **** ***/ auto 1st DES key: 5232 A317 1084 51** 2nd DES key: **** ***/ auto 2nd DES key: 1CB5 ED6A 2FB5 E5**	<b>Configure Encryption Base Key Table</b> Key Name:/ node200 1st DES key: **** ***/ auto 1st DES key: 5232 A317 1084 51** 2nd DES key: **** ***/ auto 2nd DES key: 1CB5 ED6A 2FB5 E5**
<b>Configure Encryption Profile Table</b> Mnemonic Name:/ tunnel1 Base Key Name:/ node100 Data Encapsulation Type:/ No_IV	<b>Configure Encryption Profile Table</b> Mnemonic Name:/ tunnel1 Base Key Name:/ node200 Data Encapsulation Type:/ No_IV
<b>Network Services Features Table Configuration</b> Port/Station Identifier:/ Icon-1 Data Compression Level:/ DISABLE Data Encryption Level:/ FORCE ON Encryption Profile:/ tunnel1	<b>Network Services Features Table Configuration</b> Port/Station Identifier:/ Icon-1 Data Compression Level:/ DISABLE Data Encryption Level:/ FORCE ON Encryption Profile:/ tunnel1



<b>Configure IP Interface Configuration Table</b> <b>Entry Number: 1/</b> [1] Interface Number:/ 5 [1] IP Address:/ 15.1.1.1 <b>Entry Number: 2/</b> [2] Interface Number:/ 6 [2] IP Address:/ 10.3.1.2 <b>Entry Number: 3/</b> [2] Interface Number:/ 1 [2] IP Address:/ 10.1.1.1	<b>Configure IP Interface Configuration Table</b> <b>Entry Number: 1/</b> [1] Interface Number:/ 5 [1] IP Address:/ 16.1.1.1 <b>Entry Number: 2/</b> [2] Interface Number:/ 6 [2] IP Address:/ 10.3.1.1 <b>Entry Number: 3/</b> [2] Interface Number:/ 1 [2] IP Address:/ 10.2.1.1
<b>Configure Tunnel Table</b> <b>Entry Number:1/</b> [1]Lcon No:/ 1 [1]Tunnel Source Address:/ 15.1.1.1 [1]Tunnel Destination Address:/ 16.1.1.1 [1]Tunnel Interface No:/ 6 [1]Encryption profile:/ tunnel1	<b>Configure Tunnel Table</b> <b>Entry Number:1/</b> [1]Lcon No:/ 1 [1]Tunnel Source Address:/ 16.1.1.1 [1]Tunnel Destination Address:/ 15.1.1.1 [1]Tunnel Interface No:/ 6 [1]Encryption profile:/ tunnel1
<b>Configure IP RouteTable</b> IP Network/Subnet: 10.2.1.0 IP Address Mask: 255.255.255.0 Next Hop: 10.3.1.1 Metric: 1	<b>Configure IP RouteTable</b> IP Network/Subnet: 10.1.1.0 IP Address Mask: 255.255.255.0 Next Hop: 10.3.1.2 Metric: 1

Figure 2-21. Encrypted Tunnels

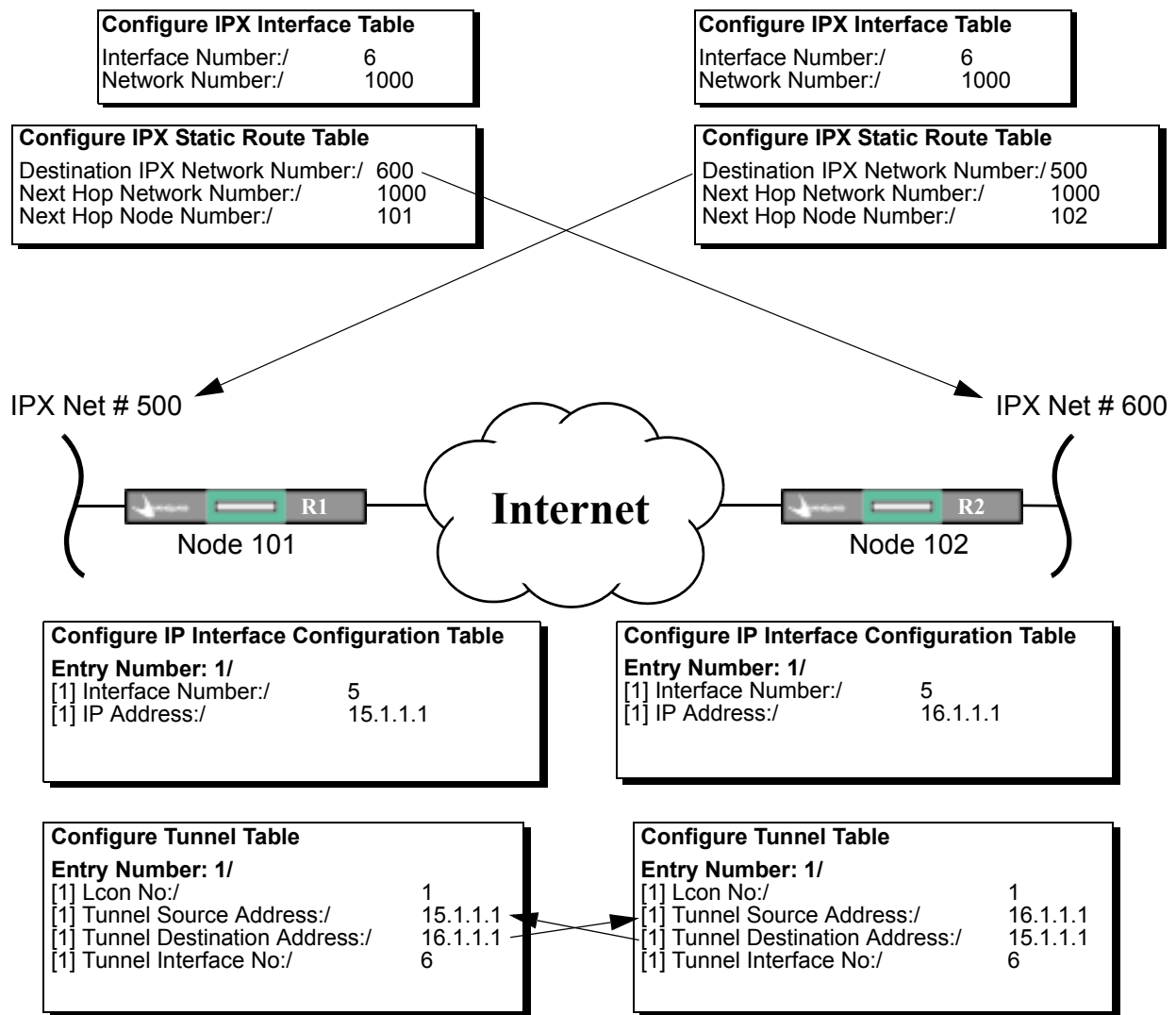
In Figure 2-21 a tunnel is configured between two routers R1 and R2. Both of them use their respective LCON interface address as the source address of the tunnel. The tunnel contains an encryption profile name. This encryption profile should be configured in the Encryption profile table. Each encryption profile contains information about the strength of the encryption, whether to use initialization vectors or not. It also points to encryption base keys. The encryption base keys on both the nodes should match for proper encryption and decryption.

**Note**

For more detailed information on encryption refer to the *Data Encryption* manual, (Part Number T0103-09).

**IPX over Tunnels**

Figure 2-22 shows the configuration required to transport IPX over tunnels.



**Figure 2-22. IPX over Tunnels**

## **Tunnel Configuration**

Two remote IPX networks (net # 500, net # 600) are connected to two remote routers. Both of these routers (R1 and R2) are connected to the Internet. It is required to transport IPX packets from net # 500 to net # 600 and vice versa.

A virtual IPX interface 6 is created with a dummy IPX net # 1000 on both the routers. This is a virtual IPX network created between the two routers. These interfaces are connected to a tunnel. The tunnel is configured with suitable source and destination addresses (15.1.1.1 and 16.1.1.1).

A static IPX routing entry is created which directs the router to forward any traffic destined to the remote network to the virtual IPX network (net # 1000). Traffic is then forwarded to the tunnel. The tunnel adds the IP and GRE header with the configured source and destination addresses and hands it over to the connected LCON for delivery.

On the remote side, the packet reaches the tunnel. The tunnel decapsulates the IP and GRE headers and gives it to IPX for forwarding to its ultimate destination.

---

VPN over LAN

Figure 2-23 shows a configuration example of VPN over LAN.

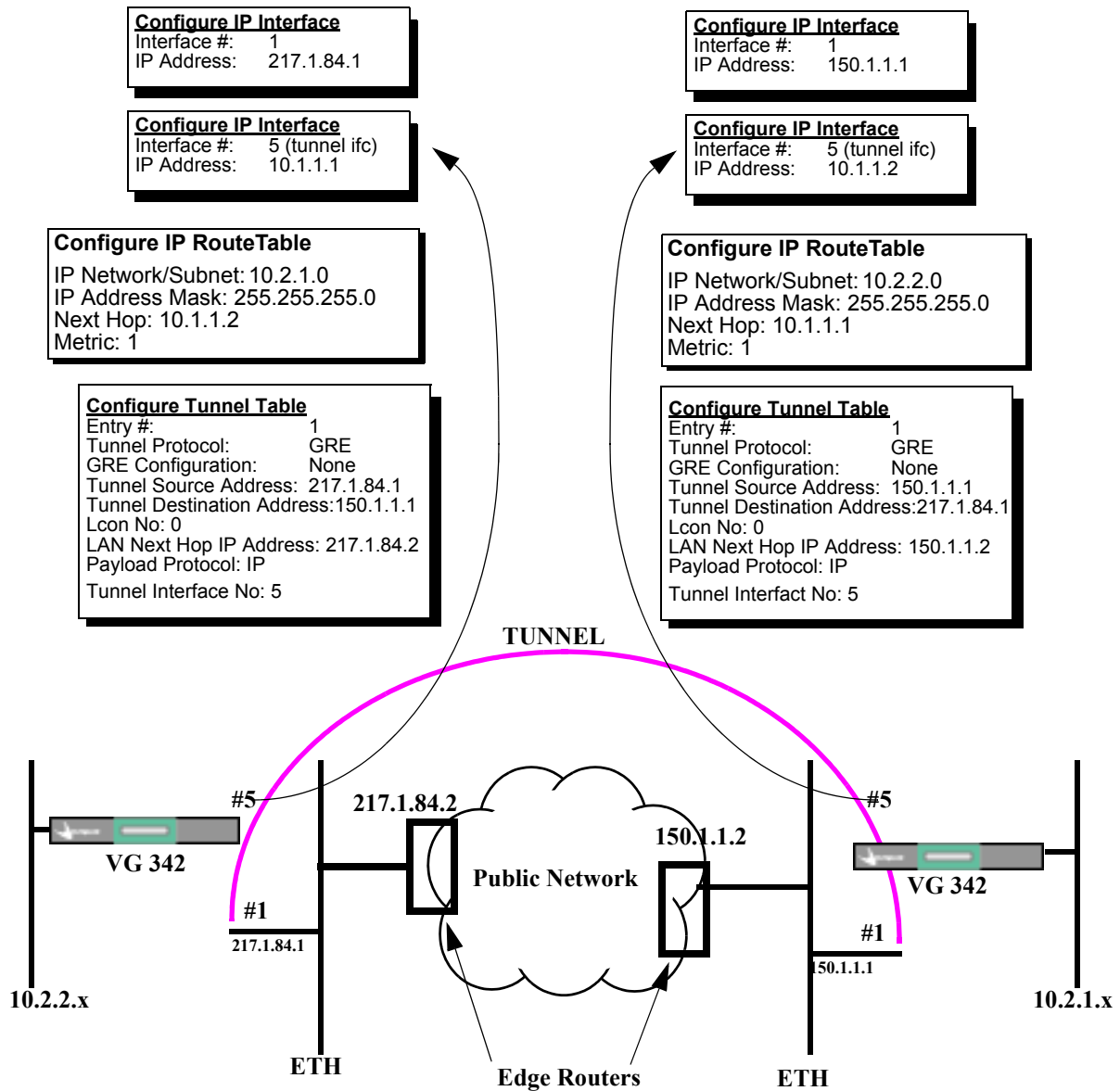
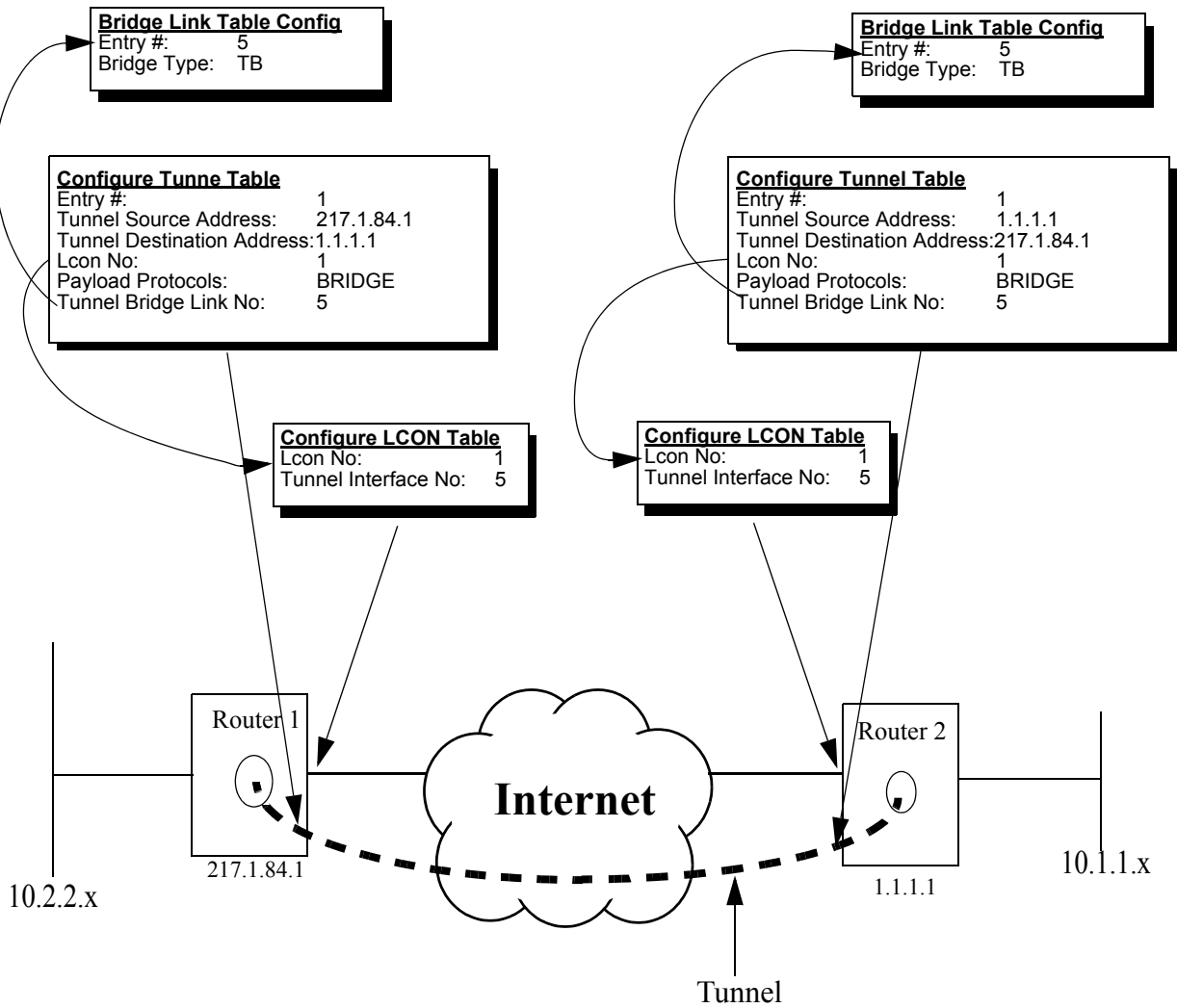


Figure 2-23. VPN over LAN Configuration Example

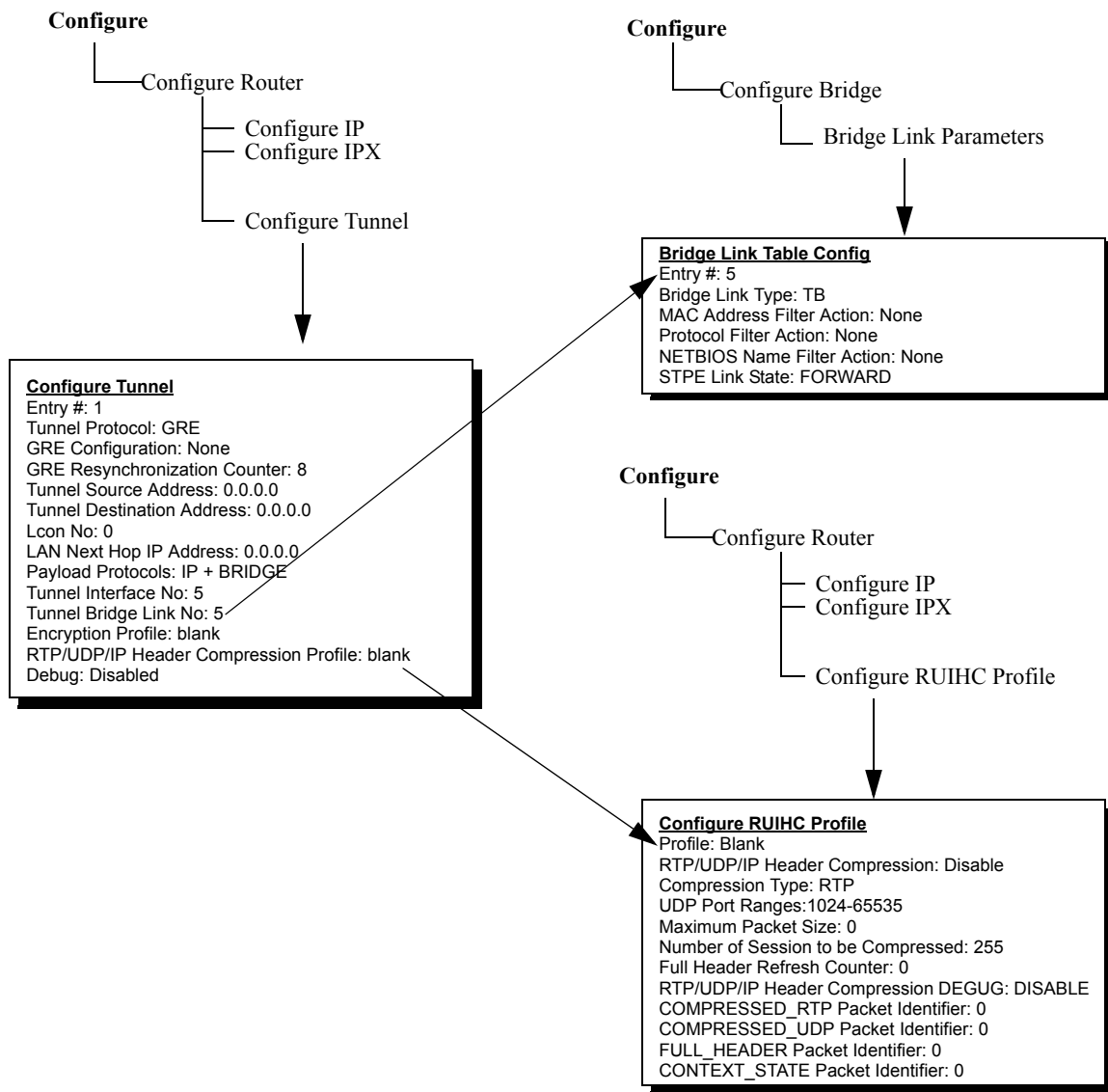
**Tunnel Supporting Bridge Traffic** Figure 2-24 shows a configuration example of a tunnel supporting bridge traffic.



**Figure 2-24. Tunnel Supporting Bridge Traffic Configuration Example**

**RTP Header Compression**

Figure 2-25 shows an example of the configuration example of a tunnel supporting RTP Header Compression.



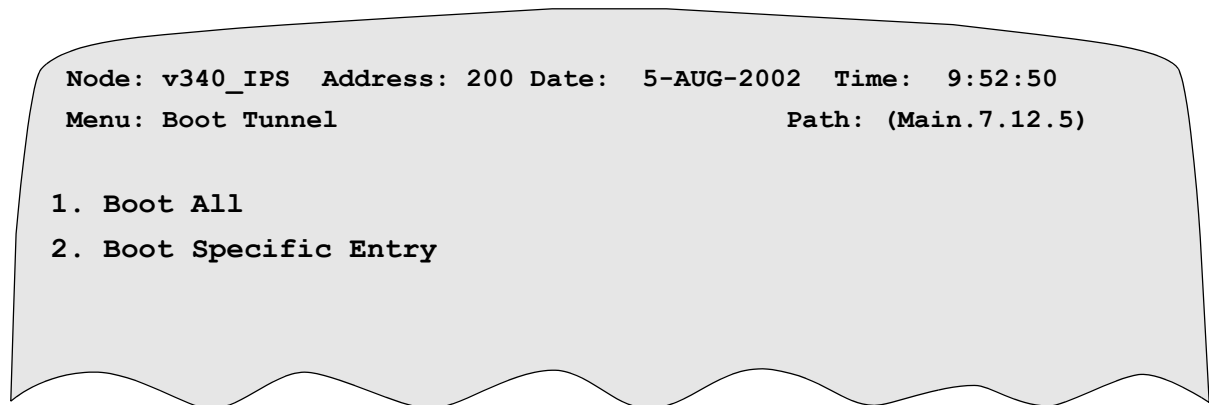
**Figure 2-25. RTP/UDP/IP Header Compression Configuration Example**

## Tunnel Boot

---

**Boot Tunnel Menu** To boot a tunnel, select Boot from the Control Terminal Port (CTP) main menu. Figure 2-26 shows an example of the Boot Tunnel Menu.

**Boot->Boot Router->Boot Tunnel->Boot All**  
**Boot->Boot Router->Boot Tunnel->Boot Specific Entry**

A screenshot of a terminal window showing the 'Boot Tunnel' menu. The terminal text includes the node name 'v340\_IPS', address '200', date '5-AUG-2002', time '9:52:50', menu name 'Boot Tunnel', and path '(Main.7.12.5)'. Below this, a numbered list shows two options: '1. Boot All' and '2. Boot Specific Entry'.

```
Node: v340_IPS Address: 200 Date: 5-AUG-2002 Time: 9:52:50
Menu: Boot Tunnel Path: (Main.7.12.5)

1. Boot All
2. Boot Specific Entry
```

**Figure 2-26. Tunnel Boot**

---

**Boot All Tunnels** Boot All tunnels boots only the tunnels which Tunnel Table configuration has changed. If the tunnel includes compression or encryption, first boot the compression or encryption feature, then boot the specific tunnel.

---

# Statistics

## Introduction

These statistics are available:

- General Tunnel Statistics
- Tunnel RTP/UDP/IP Compression Statistics
- NHS Statistics
- NHRP Mapping
- NHRP Traffic

## Examining General Tunnel Statistics

Use these steps to examine general tunnel statistics:

<b>Step</b>	<b>Action</b>	<b>Result</b>
1	Select <b>Status/Statistics</b> , from the CTP Main menu.	The Status/Statistics menu appears.
2	Select <b>Router Stats</b> .	The Router Stats menu is displayed.
3	Select <b>Tunnel Statistics</b> .	The Tunnel Statistics menu is displayed.
4	Select <b>General Tunnel Statistics</b> .	A screen similar to the one in Figure 2-27 is displayed.

```

Node: Address:                               Date:                               Time
Tunnel Statistics

Tnl  Tunnel           Tunnel           Prot  Packets  Packets  Packets  Encr  RUIHC
No.  Source            Destination      Sent   Rcvd    Dropped  Stat  Stat
-----
  1  217.1.84.28      219.1.85.2      IP     120     89      2      NA  DIS
  2  217.1.84.34      219.1.85.2      IP      56     78      7      DATA DIS
  3  217.1.84.34      219.1.85.2      IPX     68     90     10      DATA DIS
  4  217.1.84.34      219.1.86.4      BRID    12    100      2      DATA DIS
    
```

**Figure 2-27. General Tunnel Statistics**

**General Tunnel Statistics Screen Terms**

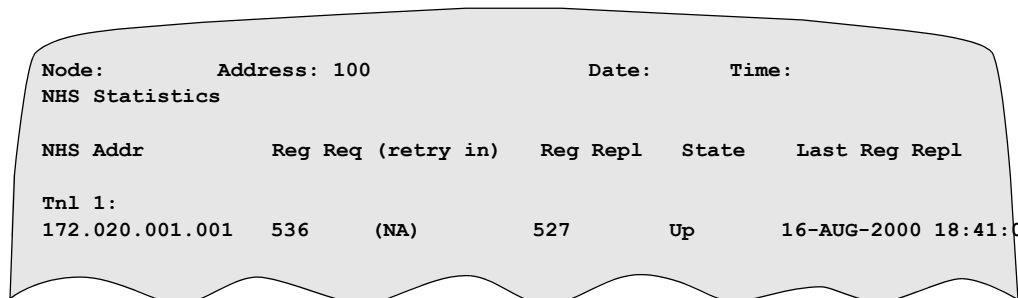
All statistics are computed since the last statistics reset or node boot. This table describes the terms displayed in Figure 2-27.

<i>Term</i>	<i>Indicates</i>
Tnl No.	Corresponds to the Entry Number of the tunnel configuration.
Tunnel Source	Corresponds to the address in the source address field of the tunnel packet.
Tunnel Destination	Corresponds to the address of the remote end of the tunnel.
Prot	Specifies the protocol type of the payload data.
Packets Sent	Indicates the number of packets sent.
Packets Rcvd	Indicates the number of packets received.
Packets Dropped	Indicates the number of packets dropped.
Encr Stat	Indicates the state of encryption.
RUIHC Stat	Indicates the state of compression.

**Examining NHS Statistics**

Use the steps below to examine NHS statistics. A sample NHS Statistics screen is shown in Figure 2-28.

<i>Step</i>	<i>Action</i>	<i>Result</i>
1	Select <b>Statistics</b> , from the CTP main menu.	The Statistics menu appears.
2	Select <b>Router Stats</b> .	The router stats menu appears.
3	Select <b>Tunnel Statistics</b> .	The Tunnel statistics menu appears.
4	Select <b>NHS Statistics</b> .	A screen similar to the one below appears.



**Figure 2-28. NHS Statistics**

**NHS Statistics  
Screen terms**

The table below describes the terms displayed in Figure 2-28.

■ **Note**

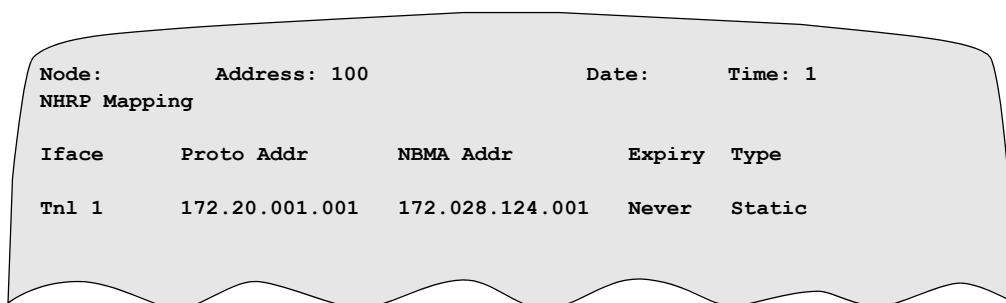
All statistics are computed since the last statistics reset or node boot.

<i><b>Term</b></i>	<i><b>Indicates</b></i>
Tnl No.	Corresponds to the entry number of the Tunnel configuration
NHS Addr	Corresponds to the IP address of the Next Hop Server.
Reg Req (retry in)	Indicates the number of registration requests sent Indicates the time left until the next registration request
Reg Repl	Indicates the number of registration replies
State	Indicates the state of the NHS connection
Last Reg Repl	Indicates the date/time of the last registration reply.

**Examining NHRP  
Mapping Statistics**

Use the steps below to examine NHRP Mapping statistics. A sample NHRP Mapping Statistics screen is shown in Figure 2-29.

<i><b>Step</b></i>	<i><b>Action</b></i>	<i><b>Result</b></i>
1	Select <b>Statistics</b> , from the CTP main menu	The Statistics menu appears
2	Select <b>Router Stats</b>	The router stats menu appears
3	Select <b>Tunnel Statistics</b>	The Tunnel statistics menu appears
4	Select <b>NHRP Statistics</b>	A screen similar to the one below appears



**Figure 2-29. NHRP Mapping Statistics**

**NHRP Mapping Statistics Screen**

The table below describes the terms displayed in Figure 2-29.

■ **Note**

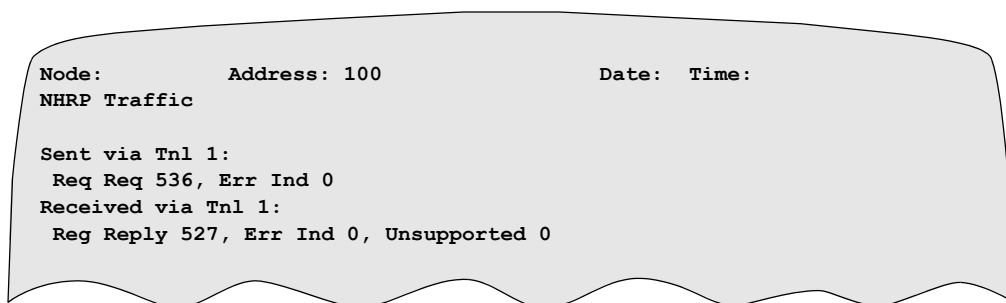
All statistics are computed since the last statistics reset or node boot.

<i><b>Term</b></i>	<i><b>Indicates</b></i>
Iface	Identifies the tunnel entry number for this NHRP mapping.
Proto Addr	Corresponds to the IP address of the Tunnel on the Next Hop Server
NBMA Addr	Corresponds to the IP address of the direct connect Next Hop to reach the NHS.
Expiry	Indicates the expiry time of the connection
Type	Indicates the type of connection to the NHS

**Examining NHRP Traffic Statistics**

Use the steps below to examine NHRP Traffic statistics. A sample NHRP Traffic Statistics screen is shown in Figure 2-30.

<i><b>Step</b></i>	<i><b>Action</b></i>	<i><b>Result</b></i>
1	Select <b>Statistics</b> , from the CTP main menu	The Statistics menu appears
2	Select <b>Router Stats</b>	The router stats menu appears
3	Select <b>Tunnel Statistics</b>	The Tunnel statistics menu appears
4	Select <b>NHRP Traffic Statistics</b>	A screen similar to the one below appears



**Figure 2-30. NHRP Traffic Statistics**

**NHRP Traffic Statistic Screen Terms**

The table below describes the terms displayed in Figure 2-30.

■ **Note**

All statistics are computed since the last statistics reset or node boot.

<b>Term</b>	<b>Indicates</b>
Sent via (eg. Tnl 1:, Tnl 2: )	Corresponds to the entry number of the Tunnel configuration
Reg Req	Indicates the number of registration requests sent
Err Ind	Indicates the number of registration requests sent in error
Received via (eg. Tnl 1:, Tnl 2: )	Indicates the time left until the next registration request
Reg Reply	Indicates the number of registration replies
Err Ind	Indicates the number of registration requests received in error
Unsupported	Indicates the number of registration requests received as unsupported



## Overview

---

### Introduction

IPSec is a widely accepted standard for protecting the integrity and confidentiality of user data when it is being transported on the Internet. The Vanguard IPSec option enables Vanguard products to create secured VPNs over a public IP network or the Internet. This chapter addresses specific Vanguard IPSec features.

---

### IPSec Overview

IPSec stands for IP Security. IPSec is defined by numerous IETF RFC's covering a large subject area. An IPSec session uses one or both of the following mechanism to protect user data during transit over an inherently insecure environment:

- Authentication Header (AH) - uses digital signature to ensure the integrity of the packet (that the packet is not forged or altered during transit).
- Encapsulated Security Payload (ESP) - uses encryption to protect the confidentiality of user data.

When the industry refers to IPSec, they are referring the various collective mechanisms available to protect user data:

- Uses ISAKMP (Internet Security Association Key Management Protocol) to negotiate and set up a secured communication channel between two IPSec peers.
- Uses IKE (Internet Key Exchange) protocol to negotiate the exchange of keying materials and provide protection between two IPSec peers.
- Uses the negotiated ESP and AH transform to protect user data for the duration of the negotiated session.

---

### IPSec Software Support

The Vanguard 340, 342, 340 Enhanced, 6435 and 6455 support IPSec capability built into the operating software with Security License for Vanguard Software Builder and requires no additional hardware.

---

### IPSec Software Support for 3400 and 6840: IPSafe

From Release 7.1.R00A, IPSafe License provides only two tunnels with IPSec and/or SAM for 3400 and 6840 with no hardware encryption card installed. When two IPSec tunnels or two SAM tunnels or one of each (i.e., 1-IPSec and 1-SAM) are configured in any tunnel table entries, the third table entry disallows a selection of IPSec or SAM. Also, no Network Service Encryptions are available with the IPSafe License. The Security License still supports Network Services Encryption and greater than two IPSec/SAM tunnels.

---

### Authentication Methods

Under IPSec, authentication of the remote peer can be accomplished with:

- Pre-shared key - The pre-shared key is shared between two IPSec peers. The key is not used directly as an encryption key. Instead, it acts as a seed to create the base keying material which then is used to create other keying materials

for encryption and authentication.

## Encryption Information

For a detailed source of information on encryption, refer to the *Data Encryption* manual, (Part Number T0103-09).

## Limitations

IPSec requires adding 80 bytes of overhead for the encapsulation. As a result, IPSec Tunnel with its associated WAN interface MTU size set to 1,500 (default) needs to fragment data when it receives more than 1,392 bytes data with DF (Don't Fragment) is set.

For example, when the host PC's MTU size is set to 1,500 (default), it can send out up to 1,472 bytes pings (i.e. 1500 – 28-byte overhead) with DF bit set (see Figure 3-1).

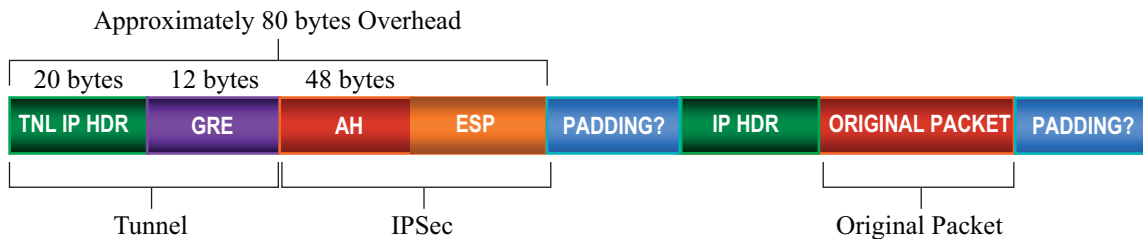
However, when the node is receiving this 1,472-byte data with DF bit set, it needs to add 80 bytes of overhead to send it through IPSec Tunnel. Therefore, 1,392 byte (i.e. 1472 – 80 = 1,392) becomes the maximum number the node can manage the data with DF bit set.

There are two workarounds to overcome this limitation. They are:

- 1 Increase the physical WAN interface's MTU size up to 1,620 and boot the node. It is important to not increase the tunnel interface because the tunnel interface is virtual. The actual data transaction is managed by the physical WAN interface.

OR

- 2 Decrease the data size with DF bit set on the host PC.



**Figure 3-1. IPsec Limitation Example**

## Vanguard IP Security

### Vanguard IPsec Implementation

---

The Vanguard IPsec implementation enables all Vanguard products that have an encryption SIMM socket on the motherboard to have IPsec support. The implementation uses the encryption engine on the encryption SIMM to perform DES, Triple DES or Triple DES and AES encryption of the user data. Hashing is used to calculate the message digest for the authentication header or ESP authentication.

---

### Vanguard IPsec Implementation Characteristics

The following are characteristics of the Vanguard IPsec/VPN implementation:

- For each remote site that the node is required to talk to, an IPsec tunnel interface is permanently created. Resources for the interface are tied-up even though there cannot be any traffic passing between the remote site and the local node. An IPsec tunnel is created for an IP Interface via the tunnel sub-menu under IP Router. Other tunnel characteristics include:
  - A tunnel requires another IP interface to connect to an LCON for accessing a particular WAN link.
  - Multiple tunnels to different remote sites can flow through the same LCON.
  - Each tunnel interface must have its own numbered IP address.
  - Tunnels can be setup over LAN Interfaces.

#### ■ Note

The tunnel interface can also use unnumbered IP addresses. It is not always necessary to configure static routes to the VPN site. RIP can be used to transfer routes from one VPN endpoint to the other VPN endpoint. However, care should be taken when using the rip route control feature so that these routes to private networks are not inadvertently sent to the Internet routers.

- An incoming IPsec connection negotiation is processed only if the interface to the calling node is configured in the node.
- Static routes must be configured for the tunnel between the two sites.

## Modifications for IPSec

The Examine, List, Copy, Boot and Delete functions are standard commands that have been extended to support IPSec. Security restriction makes it necessary to implement some functional modifications for Data Encryption. In the table below “Yes” indicates that the Vanguard router supports the operation, and a “No” indicates the Vanguard Router does not support the operation. Some restrictions do apply as described following the table:

<b>Operation</b>	<b>IPSec Profile Parameters</b>	<b>ISAKMP Policy</b>	<b>IPSec Transform Set</b>	<b>ISAKMP Preshared Key</b>
Examine	Yes	Yes	Yes	<sup>1</sup> Yes
List	Yes	Yes	Yes	<sup>1</sup> Yes
Copy	No	No	No	No
Boot	Yes	Yes	Yes	Yes
Delete	Yes	Yes	Yes	<sup>2</sup> Yes

### ■Note

<sup>1</sup> The Preshared Key Tables may be seen, but the actual key values are not displayed for security reasons.

<sup>2</sup> The Preshared keys can be deleted one by one, or all at once.

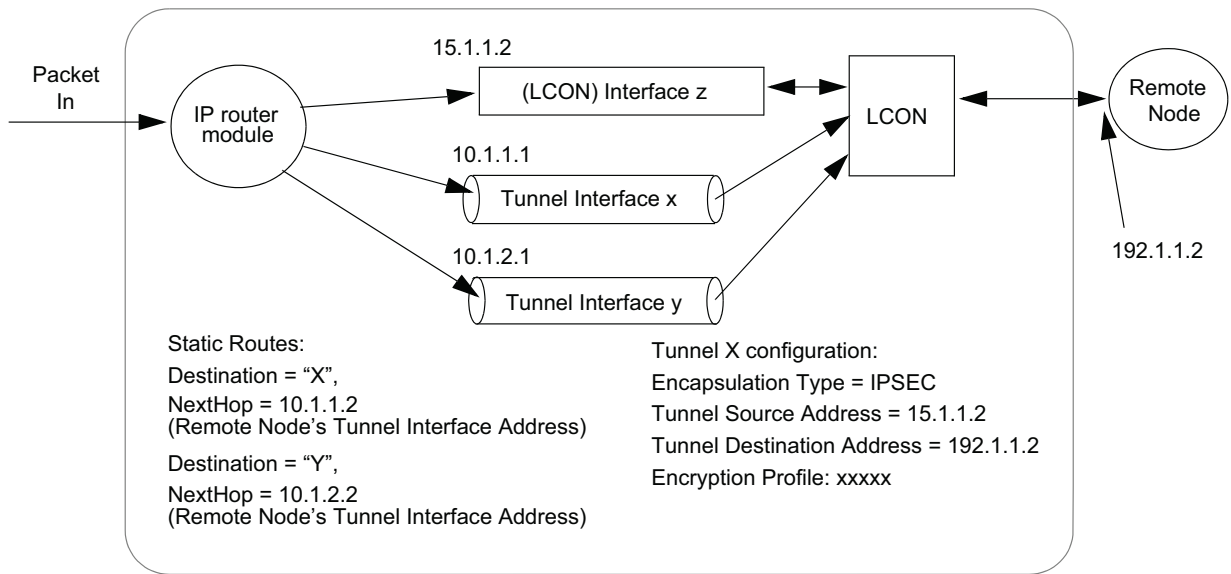
## Third Party Support

The ability to interoperate with third party IPSEC equipment is important to Vanguard Networks. The Vanguard Networks Routers are able to interoperate with the Third Party IPSEC implementation using the following algorithms and negotiation options:

- Authentication using Pre-shared Keys
- Authentication Header using HMAC-MD5-96, or HMAC-SHA-1-96
- Encapsulating Security Payload (ESP) using DES, Triple DES, and AES with an ECC DIMM or an Advanced Encryption Card (AEC) installed in the node. When using the DCC SIMM, Vanguard Networks only supports ESP when using DES (in order to interoperate with a Third Party).
- ESP with Authentication using HMAC-MD5-96 or HMAC-SHA-1-96
- Anti-replay Sliding Window
- MODP Groups 1 and 2
- Perfect Forward Secrecy
- SA Life Time and Character Limit

**Site-to-Site IPSec VPN Example**

Figure 3-2 shows a typical example of a Vanguard site-to-site IPSec VPN.



**Figure 3-2. Site-to-Site IPSec VPN Example**

# IPSec Configuration

## Introduction

Follow these steps to access IPSec from the Network Security Menu:

Step	Action	Result
1	Select <b>Configure</b> , from the CTP Main menu.	The Configure menu appears.
2	Select <b>Configure Network Security</b> .	The Configure Network Security Menu is shown.
3	Select <b>Configure IPSec</b> .	

```

Node: v342-1      Address: (blank)      Date: 12-APR-2004  Time:
15:02:09
Menu: Configure Network Security      Path: (Main.6.18)

1. Configure Encryption
2. Configure IPSec
3. Configure Digital Certificate
    
```

**Figure 3-3. Configure Network Security**

Figure 3-4 illustrates the IPSec configuration tables under the Configure IPSec menu.

```

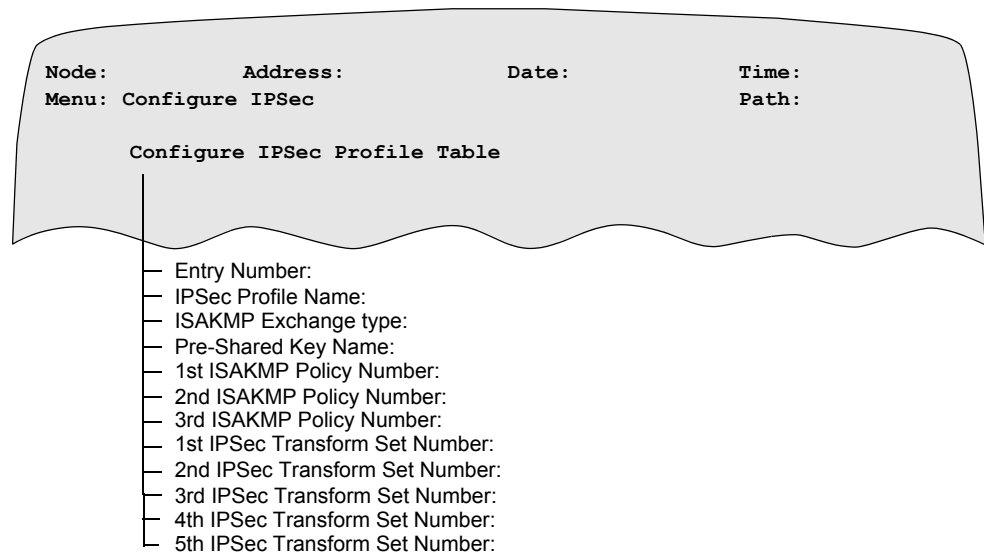
Node:      Address:      Date:      Time:
Menu: Configure IPSec      Path:

- IPSec Profile Table
- ISAKMP Policy Table
- IPSec Transform Set Table
- ISAKMP Preshared Key Table
    
```

**Figure 3-4. IPSec Configuration Tables**

## IPSec Profile Table Parameters

Figure 3-5 illustrates the IPSec Profile Table configuration parameters.



**Figure 3-5. IPSec Profile Table Parameters**

## Parameters

These are the parameters that must be configured in the IPSec Profile Table.

### Entry Number

Range	1 to 64
Default	1
Description	Entry number used to reference this table record.
Boot Type:	Boot IPSec Profile Table.

### IPSec Profile Name

Range	1 - 15 alphanumeric characters. Use the spacebar to blank field.
Default	(blank)
Description	The name of this IPSec profile. This is the profile name entered during tunnel configuration in the Configure Tunnel Table menu.
Boot Type:	Boot IPSec Profile Table.

### ISAKMP Phase 1 Exchange Type

Range	MAIN_MODE, AGGRESSIVE MODE
Default	MAIN_MODE

### ISAKMP Phase 1 Exchange Type

Description	ISAKMP Phase 1 exchange type: Main Mode - More secure option; generally preferred. Aggressive Mode - Less secure option. Used with dynamic local addressing it is necessary for interoperability with some VPN concentrators.
Boot Type:	Boot IPSec Profile Table.

### Pre-Shared Key Name

Range	1-17 alphanumeric characters. Use the spacebar to blank field.
Default	(blank)
Description	The name of the pre-shared key to be used to authenticate the remote peer. (Valid if the selected ISAKMP policy specifies pre-shared key.)
Boot Type:	Boot IPSec Profile Table.

### ISAKMP Policy Number (1st, 2nd, 3rd, etc)

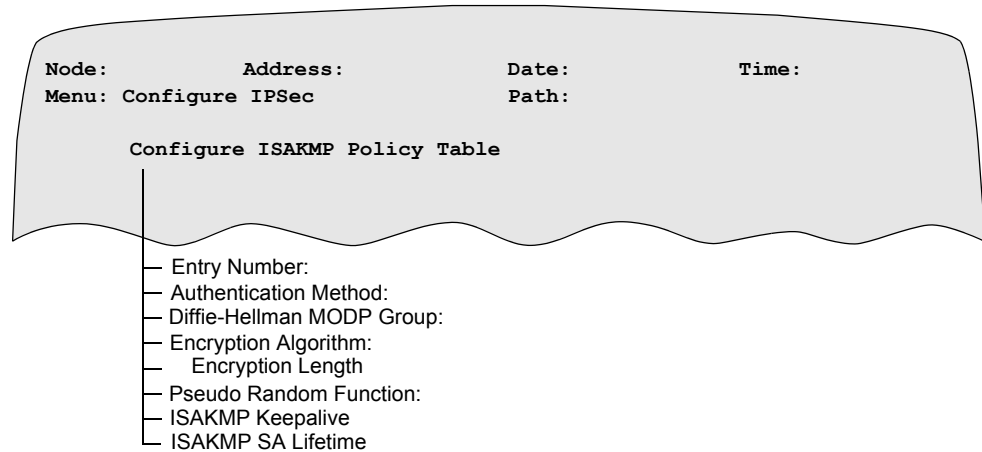
Range	1 to 10
Default	1
Description	The ISAKMP Policies are passed in the Security Association (SA) Proposal Payloads negotiated with the remote peer. The entry number selected must be configured in the ISAKMP Policy Table.
Boot Type:	Boot IPSec Profile Table.

### IPSec Transform Set Number (1st, 2nd, 3rd, 4th and 5th)

Range	1 to 10
Default	1
Description	The entry number from the IPSec Transform Set Table. The selected entry number must be configured in the IPSec Transform Set Table.
Boot Type:	Boot IPSec Profile Table.

### ISAKMP Policy Table Parameters

Figure 3-6 illustrates the ISAKMP Policy Table configuration parameters.



**Figure 3-6. ISAKMP Policy Table Parameters**

## Parameters

These are the parameters that must be configured in the ISAKMP Policy Table:

### Entry Number

Range	1 to 10
Default	1
Description	Entry number used to reference this table record.
Boot Type:	Boot IPSec Policy Table.

### Authentication Method

Range	PRE-SHARED_KEY, RSA_SIGNATURE
Default	PRE-SHARED_KEY
Description	The ISAKMP SA authentication method.
Boot Type:	Boot IPSec Policy Table.

### Diffie-Hellman MODP Group

Range	1 or 2
Default	1
Description	1 for 768 bits or 2 for 1,024 bits group.
Boot Type:	Boot IPSec Policy Table.

**Encryption Algorithm**

Range:	DES_CBC, 3DES_CBC, AES_CBC
Default	DES_CBC
Description	<p>The encryption algorithm that protects the ISAKMP exchange. The Encryption Algorithm range of values depends on the SIMM/DIMM installed in the node.</p> <ul style="list-style-type: none"> <li>• DES SIMM - DES_CBC, 3DES_CBC</li> <li>• 3DES SIMM - DES_CBC, 3DES_CBC</li> <li>• ECC DIMM / Advanced Encryption Module - DES_CBC, 3DES_CBC, AES_CBC</li> </ul> <p>■ <b>Note</b> The Vanguard 342 supports AES in Release 6.3 and greater with an ECC DIMM installed in the node, Release 6.4 and greater supports the Vanguard 340 Enhanced. Release 6.4 and greater supports the 7300 Advanced Encryption Card.</p>
Boot Type:	Boot IPSec Policy Table.

**Encryption Length**

Range	128, 192, 256
Default	128
Description	<p>Supported Advanced Encryption Standard (AES) lengths are: 128, 192 and 256 bits.</p> <p>■ <b>Note</b> This parameter is displayed only if AES_CBC is chosen for the Encryption Algorithm with an ECC DIMM or an Advanced Encryption Card installed in the node.</p>
Boot Type:	Boot IPSec Policy Table.

**Pseudo Random Function**

Range	MD5, SHA-1
Default	MD5
Description	The Pseudo Random Function used for authentication and for deriving the keying material used by the encryption algorithm.
Boot Type:	Boot IPSec Policy Table.

**ISAKMP SA Lifetime**

Range	5 to 525,600
-------	--------------

**ISAKMP SA Lifetime**

Default	1440
Description	The ISAKMP SA Lifetime in minutes. (1440 minutes = 24 hours, 525,600 minutes = 1 year).
Boot Type:	Boot IPSec Policy Table

**ISAKMP Keepalive Idle Time**

Range:	0 to 3600
Default:	30
Description:	The ISAKMP KeepAlive Idle interval specifies the minimum amount of time (in seconds) the peer is inactive before sending a keepalive message. If packets have not been received from the peer for the duration of the ISAKMP Keepalive idle time then a keepalive message is sent to the peer. 0 seconds disables the sending of ISAKMP keepalive messages.
Boot Type:	Boot IPSec Policy Table.

**■ Note**

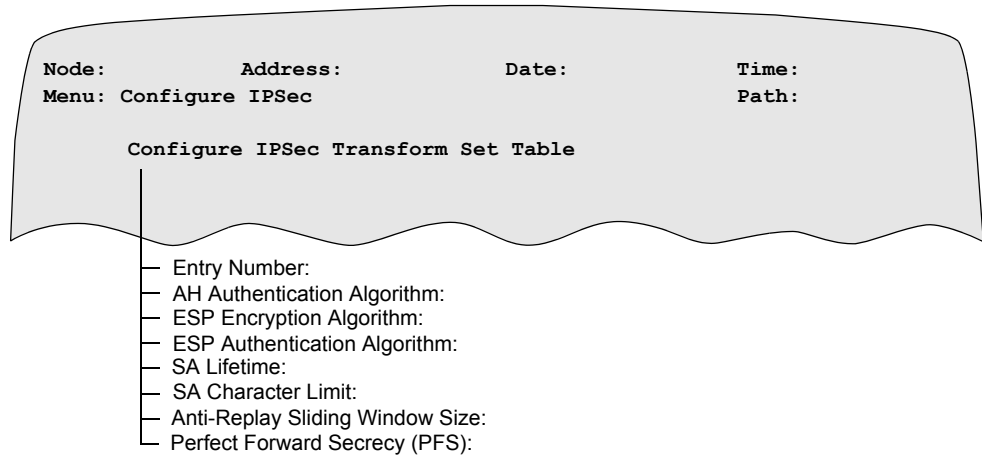
Even with ISAKMP keepalive disabled, the node will respond to ISAKMP keepalive messages received from peers.

**ISAKMP Keepalive Retry Interval**

Range:	5 to 60
Default:	5
Description:	The ISAKMP KeepAlive retry interval specifies the amount of time (in seconds) before a keepalive message is resent when no reply has been received from the peer.
Boot Type:	Boot IPSec Policy Table.

**IPSec Transform Set Table Parameters**

Figure 3-7 illustrates the IPSec Transform Set Table configuration parameters.



**Figure 3-7. IPSec Transform Set Table Parameters**

**Parameters**

These are the parameters that must be configured in the IPSec Transform Set Table.

**Entry Number**

Range	1 to 10
Default	1
Description	Entry number used to reference this table record.
Boot Type:	Boot IPSec Policy Table.

**AH Authentication Algorithm**

Range	NONE, MD5_HMAC, SHA_HMAC
Default	NONE
Description	Supported authentication algorithms: HMAC-MD5-96 (RFC-2403) and HMAC-SHA-1-96 (RFC-2404). When choosing NONE, no AH transform is applied to the packet.
Boot Type:	Boot IPSec Transform Set Table.

**ESP Encryption Algorithm**

Range	NONE, NULL, DES_CBC, 3DES_128, 3DES_CBC, AES_CBC
Default	DES_CBC

**ESP Encryption Algorithm**

Description	<p>Supported encryption algorithms: DES_CBC (RFC-2405), 3DES_128 (128 bits key), 3DES_CBC, AES_CBC, NULL (RFC-2410), and NONE</p> <p>The ESP Encryption Algorithm range of values depends on the SIMM/DIMM installed in the node.</p> <ul style="list-style-type: none"> <li>• DES SIMM - NONE, NULL, DES_CBC</li> <li>• 3DES SIMM - NONE, NULL, DES_CBC, 3DES_128</li> <li>• ECC DIMM or Advanced Encryption Module- NONE, NULL, DES_CBC, 3DES_128, 3DES_CBC, AES_CBC</li> </ul> <p>When choosing NONE, no ESP transform is applied to the packet.</p> <p><b>■Note</b> The Vanguard 342 supports AES in Release 6.3 and greater with an ECC DIMM installed in the node, Release 6.4 and greater supports the Vanguard 340 Enhanced. The Vanguard 7300 Series Advanced Encryption Card is supported in Release 6.4 and greater.</p>
Boot Type:	Boot IPSec Transform Set Table.

**Key Length**

Range	128, 192, 256
Default	128
Description	<p>Supported AES encryption lengths are: 128, 192, and 256 bits.</p> <p><b>■Note</b> This parameter is displayed only if AES_CBC is chosen for the ESP Encryption Algorithm range. The Vanguard 342 supports AES in Release 6.3 and greater with an ECC DIMM installed in the node, Release 6.4 and greater supports the Vanguard 340 Enhanced. The Vanguard 7300 Series Advanced Encryption Card is supported in Release 6.4 and greater.</p>
Boot Type:	Boot IPSec Transform Set Table.

**ESP Authentication Algorithm**

Range	NONE, MD5_HMAC, SHA_HMAC
Default	NONE
Description	Supported authentication algorithms: HMAC-MD5-96 (RFC-2403) and HMAC-SHA-1-96 (RFC-2404).
Boot Type:	Boot IPSec Transform Set Table.

**SA Life Time**

Range	5 to 525,600
Default	1440
Description	Specifies IPSec SA lifetime in minutes. (1440 minutes = 24 hours. 525,600 minutes = 1 year).
Boot Type:	Boot IPSec Transform Set Table.

**SA Character Limit**

Range	0 or 5,000 to 4,000,000
Default	0
Description	The maximum number of kilo-bytes of user data allowed to be transferred under the protection of this SA. Set value to zero to disable this feature.
Boot Type:	Boot IPSec Transform Set Table.

**Anti-Replay Sliding Window Size**

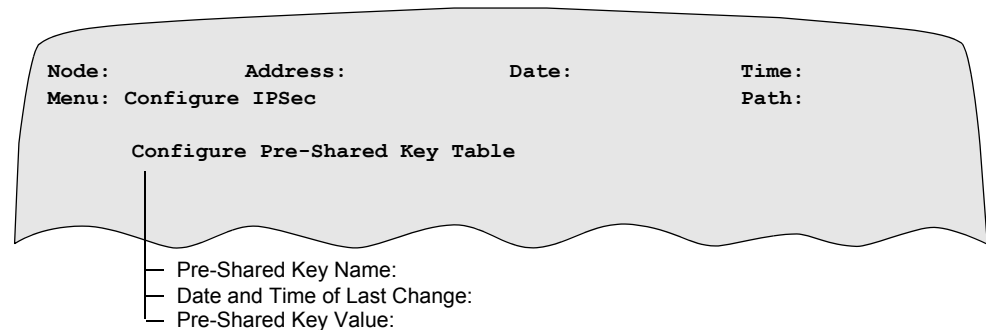
Range	0 or 32
Default	0
Description	The anti-replay packet sequence checking window size. Any received packet outside the sliding window is discarded. Set the size to 32 to enable Anti-Replay, 0 to disable the feature.
Boot Type:	Boot IPSec Transform Set Table.

**Perfect Forward Secrecy (PFS)**

Range	Disable, Enable
Default	Disable
Description	Enable Perfect Forward Secrecy for ISAKMP Phase2 (Quick Mode). Each set of Phase 2 exchanges is protected by different D-H Exchange.
Boot Type:	Boot IPSec Transform Set Table.

**Pre-Shared Key Table Parameters**

Figure 3-8 illustrates the Pre-Shared Key Table configuration parameters. The entries in the Pre-Shared Key Table are encrypted using the node key and are stored in CMEM similar to the base key table.



**Figure 3-8. Pre-Shared Key Table Parameters**

**Parameters**

These are the parameters that must be configured in the Pre-Shared Key Table.

**Entry Number**

Range	1 to 10
Default	1
Description	Entry number used to reference this table record.
Boot Type:	Boot ISAKMP Pre-Shared Key Table

**Preshared Key Name**

Range	1-17 alphanumeric characters. Use the spacebar to blank field.
Default	(blank)
Description	Name of the pre-shared secret key from the ISAKMP Policy Table when the Pre-Shared Key Authentication Method is selected.
Boot Type:	Boot ISAKMP Pre-Shared Key Table

**Preshared Key Value**

Range	1 to 20 alphanumeric characters
Default	(blank)
Description	Value of the Pre-Shared Key comprised of any string of ASCII characters.
Boot Type:	Boot ISAKMP Pre-Shared Key Table

**Date and Time of Last Change**

Range	(real time)
Default	1-JAN-2000 0:00:00
Description	The date and time of the last key change. Read only parameter that is automatically filled in by the system when key is saved.
Boot Type:	Boot ISAKMP Pre-Shared Key Table

---

## IPSec Configuration Example

### IPSec Example

Figure 3-9 shows an example of IPSec configuration.

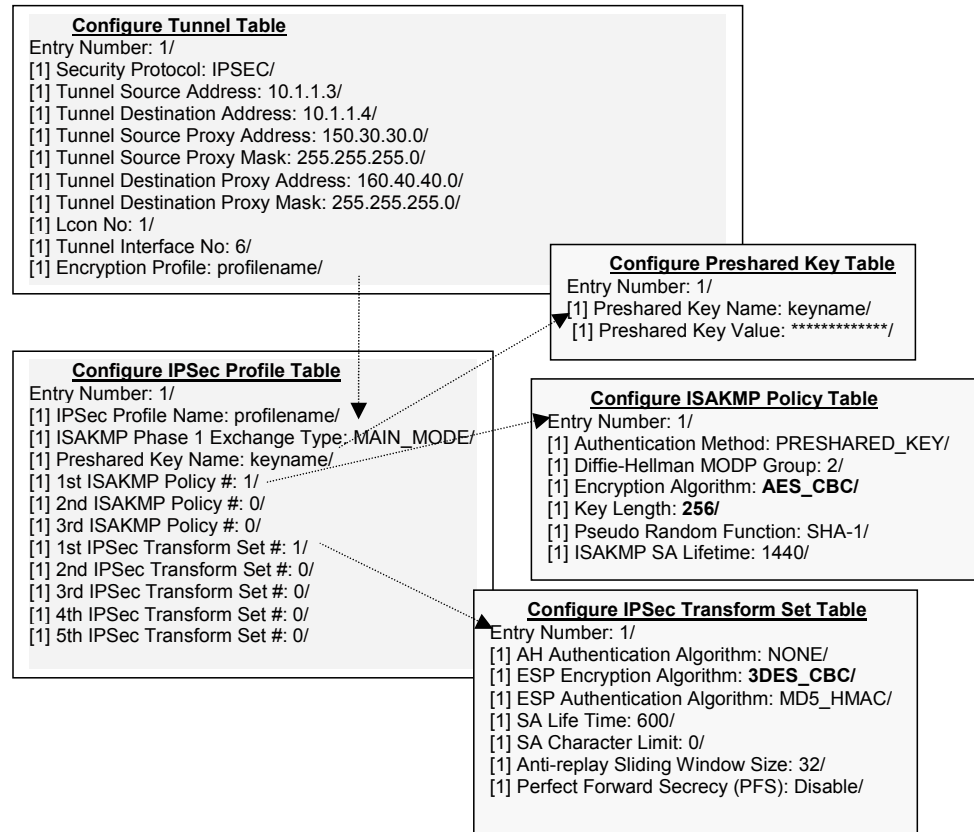
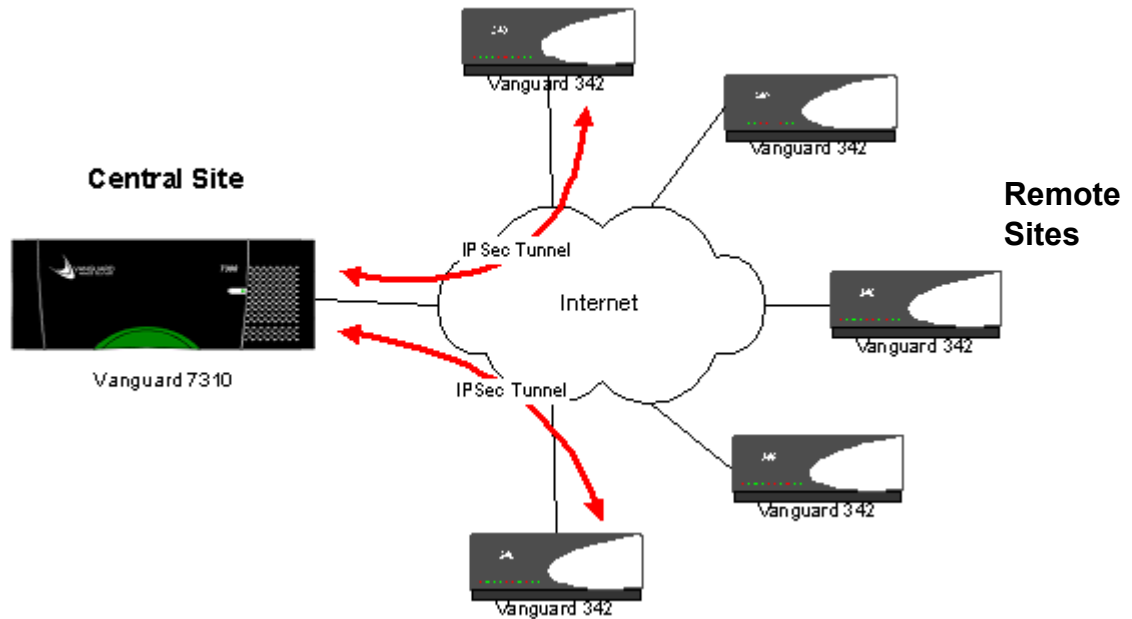


Figure 3-9. IPSec Configuration Example

**Vanguard 7300  
IPSec Tunnel**

Figure 3-10 shows a configuration that illustrates a central site solution where a Vanguard 7310 would terminate multiple IPSec tunnels to remote sites.



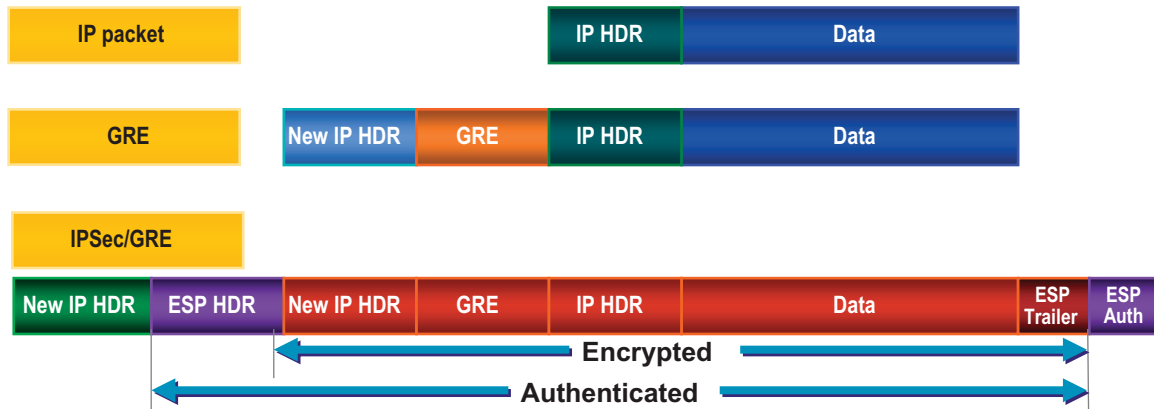
**Figure 3-10. Central Site Example**

## GRE\_IPSec Example

### Introduction

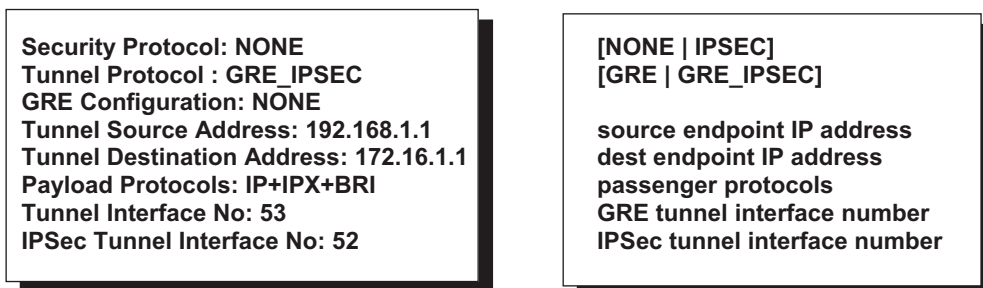
To overcome the limitations in IPSec standard, GRE\_IPSec uses GRE tunnels in conjunction with IPSec, which only supports IP traffic and not multicast and broadcast.

GRE tunnels with IPSec can provide multi-protocol support, multicast, broadcast, routing protocols over tunnels using IPSec standard and encryption (Figure 3-11). This traffic is encapsulated in a GRE packet prior to the IPSec encapsulation. Figure 3-12 shows a configuration example of GRE\_IPSec.



■ **Note:** GRE\_IPSec Configuration GRE\_IPSec is configurable only when Security Protocol is configured as NONE.

#### • Configure > Configure Router > Configure Tunnel



**Figure 3-11. Feature Encapsulation**

## IPSec Configuration

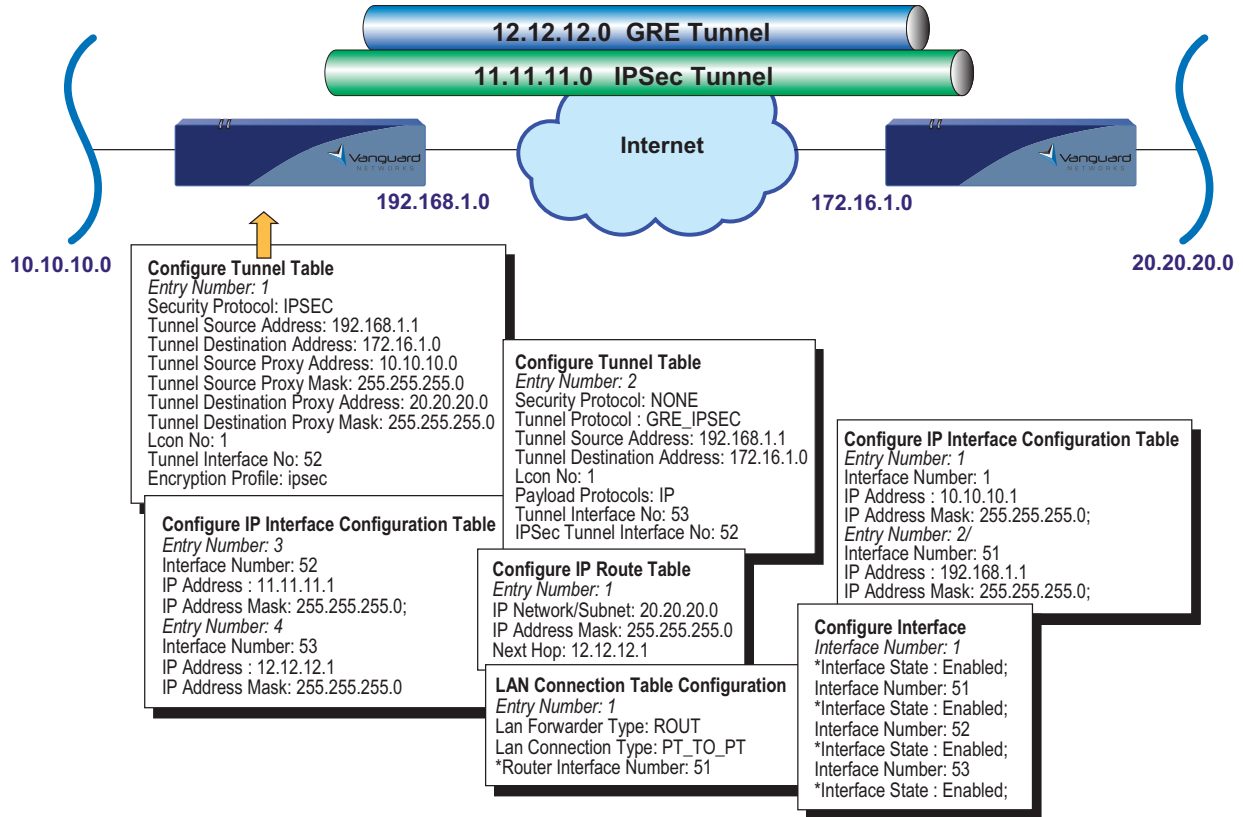


Figure 3-12. GRE\_IPSEC Configuration

## ISAKMP Aggressive Mode

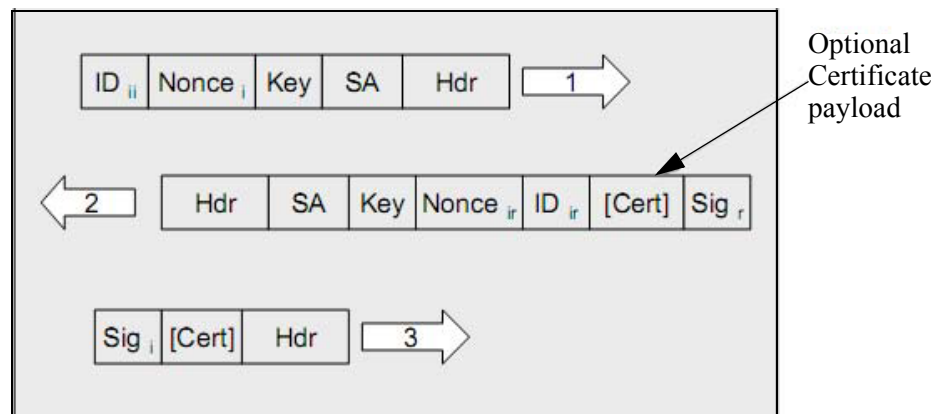
### Overview

When the Juniper SSG router is configured to accept VPNs from peers with unknown IP addresses, they requires the ISAKMP Phase 1 negotiation to be in Aggressive mode and have a Peer ID to identify the remote peer.

Vanguard implemented Aggressive Mode with the ability to specify a Peer identifier for compatibility with the Juniper SSG family.

### ISAKMP Aggressive Mode

Figure 3-13 shows the ISAKMP Aggressive Mode exchanges to complete Phase 1. Aggressive Mode offers a fast alternative to main mode exchanges (for ISAKMP Phase 1 negotiation) if the identity of the end user/host does not need to be protected. The Aggressive mode exchange consists of three messages as shown below. Message 1 and 3 are from the Initiator, and message 2 from the Responder.



**Figure 3-13. ISAKMP Aggressive Mode Exchanges**

### ISAKMP Configuration

ISAKMP can be accessed from the Control Terminal Ports (CTP) Main Menu:

**Configure > Configure Network Security > Configure IPSec > IPSec Profile Table**

### Configure IPSec Profile Table

**Entry Number: 1**  
**IPSec Profile Name: Blank**  
**ISAKMP Phase 1 Exchange Type:**

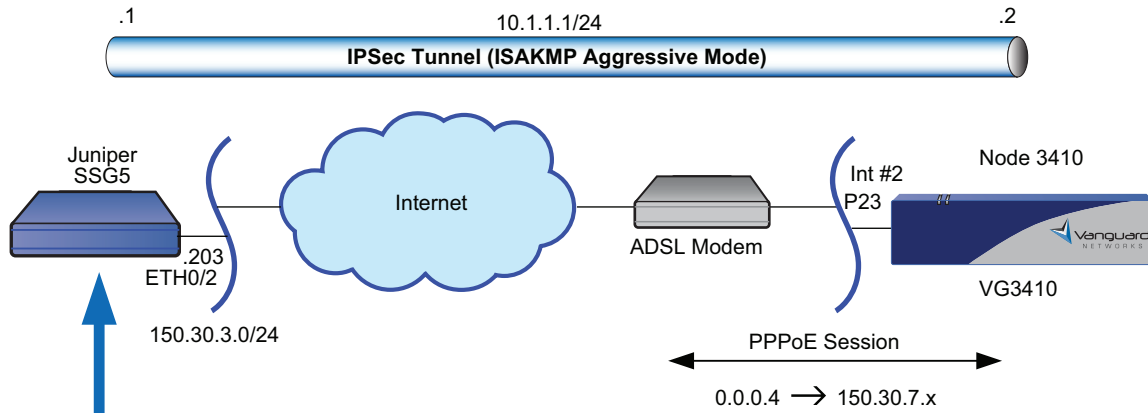
Range	MAIN_MODE, AGRESSIVE_MODE
Default	MAIN MODE
Description	Main Mode - More secure option; generally preferred. Aggressive Mode - Less secure option. Used with dynamic local addressing it is necessary for interoperability with some VPN concentrators.

**Preshared Name: Blank**  
**1st IPSec Transform Set #: 1**  
**ISAKMP Username ID: (blank)**

Range	1-63 alphanumeric characters, use the space character to blank field
Default	blank
Description	ISAKMP ID payload identifier. This parameter is required, when configured for 'Aggressive' Phase I key change mode. Both U-FQDN and FQDN are supported.



## IPSec Configuration



```
set interface ethernet0/2 ip 150.30.3.203/24
set interface tunnel.1 ip 10.1.1.1/24
set interface tunnel.1 mtu 1500
set ike p1-proposal "OHIP_Test_P1" preshare group1 esp 3des md5 hour 24
set ike p2-proposal "OHIP_Test_P2" no-pfs esp 3des sha-1 hour 8
set ike gateway "test" address 0.0.0.0 id "vanguard" Aggr outgoing-interface
"ethernet0/2" preshare 123 proposal "OHIP_Test_P1"
set vpn "test" gateway "LEAH" no-replay tunnel idletime 0 proposal "OHIP_Test_P2"
set vpn "test" id 0x3 bind interface tunnel.1
set vpn "test" proxy-id local-ip 1.1.1.1/24 remote-ip 2.2.2.2/24 "ANY"
set route 0.0.0.0/0 interface ethernet0/2 gateway 150.30.3.1
set route 192.168.2.0/24 interface tunnel.1 gateway 10.1.1.2
```

**ISAKMP Aggressive Mode Configuration Example 2**

## Statistics

### Introduction

These statistics are available:

#### Main->Status/statistics->Network Security Stats->IPSec Statistics

- IPSec Channel Statistics
- IPSec All Channel Statistics
- IPSec Summary Statistics

### IPSec Channel Statistics

Figure 3-15 shows the IPSec Channel Statistics.

```

Node: 7310      Address: 100      Date: 29-MAR-2004  Time: 16:24:58
Detailed IPSec Channel Statistics:  Channel 1      Page: 1 of 1

Channel State:                DATA
Source IP Address:            192.168.1.25 (Tunnel 2)
Destination IP Address:       192.168.1.27
IPSec Profile Name:           ipsec
Preshared Key      <ipsec>     10-MAR-2004 14:28:10
ISAKMP Protection:           3DES, SHA-1, PSK, MODP 2
ISAKMP SA Lifetime (current, limit): 4, 5 min
AH Protection:                SHA-1
ESP Protection:                3DES, MD5
IPSec SA Lifetime (current, limit): 9, 10 min
IPSec SA Char Count (current, limit): 0, 0 KBytes
IPSec Options:                AR
ISAKMP, IPSEC Neg. Failures: 0, 0
Packets Processed (sent, received): 0, 0

Packets Dropped
Encrypt, Decrypt Failures:    0, 0
Invalid SPI, Authentication, AReplay: 0, 0, 0
Last Statistics Reset:        29-MAR-2004 16:24:37

Press any key to continue ( ESC to exit ) ...

```

**Figure 3-15. IPSec Channel Statistics**

### IPSec Channel Statistics Screen Terms

Below are the screen terms used in the IPSec Channel Statistics menu:

<b>Term</b>	<b>Description</b>
Channel State	<p>INIT - Trying to establish ISAKMP SA with remote. ISAKMP Successfully negotiated ISAKMP SA with remote peer.</p> <p>DATA - Successfully established ESP and AH with remote peer, user data passing is enabled.</p> <p>NONE - Authentication Header not negotiated.</p> <p>MD5 HMAC-MD5_96 is selected as hash algorithm for the authentication header.</p> <p>SHA HMAC-SHA_1_96 is selected as hash algorithm for the authentication header.</p>
Source Channel	Identifies the Source's IP address (with tunnel no.)
Destination Channel	Identifies the Destination's IP address
IPSec Profile Name	Profile associated with this IPSec channel.
Preshared Key	Refers to the name of the pre-shared key that is being used.
ISAKMP Protection	<p>All protection schemes negotiated to protect the ISAKMP transactions. The possible combinations are listed below:</p> <p>Authentication Method:</p> <ul style="list-style-type: none"> <li>• PSK - Preshared Key</li> <li>• RSA-SIG RSA Signatures</li> </ul> <p>Encryption Algorithm:</p> <ul style="list-style-type: none"> <li>• DES</li> <li>• 3DES</li> <li>• AES_128 or AES_192 or AES_256</li> </ul> <p>Hashing Algorithm:</p> <ul style="list-style-type: none"> <li>• MD5</li> <li>• SHA</li> </ul> <p>Oakley Group:</p> <ul style="list-style-type: none"> <li>• MODP 1</li> <li>• MODP 2</li> </ul> <p>ISAKMP Keepalive:</p> <ul style="list-style-type: none"> <li>• DPD (Dead Peer Detection) This parameter appears only if the node is configured to send keepalives and the peer supports keepalives.</li> </ul>

<b>Term</b>	<b>Description</b>
ISAKMP SA Lifetime	Indicates how long the SA is valid for.
AH Protection	The Authentication Header protection in use on this channel. The possible combinations are listed below: NONE: Authentication Header not negotiated. Hashing Algorithm <ul style="list-style-type: none"> <li>• MD5_HMAC-MD_96 is selected as the hash algorithm for the authentication header.</li> <li>• SHA_HMAC-SHA_1_96 is selected as the hash algorithm for the authentication header.</li> </ul>
ESP Protection	The ESP encryption and authentication used on this channel. The possible combinations are listed below: Encryption Algorithm: <ul style="list-style-type: none"> <li>• DES</li> <li>• 3DES or 3DES_128</li> <li>• AES_128 or AES_192 or AES_256</li> </ul> Hashing Algorithm <ul style="list-style-type: none"> <li>• MD5</li> <li>• SHA</li> </ul>
IPSec SA Time Limit (Min)	Indicates how long the SA is valid for
IPSec SA Char Count (Kbytes)	Indicates the number of kilobytes that have been transferred under the protection of this SA.
IPSec Options	<ul style="list-style-type: none"> <li>• AR Anti Replay</li> <li>• PFS Perfect Forward Secrecy</li> </ul>
ISAKMP, IPSEC Neg. Failures	The number of authentication failures that have occurred on this channel.
Packets Processed (sent, received)	The number of packets that have successfully passed through the channel.

<b>Term</b>	<b>Description</b>
Packets Dropped	<p>The number of packets that have been discarded over the IPSec channel.</p> <ul style="list-style-type: none"><li>• Encrypt - Packets dropped during encryption processing errors.</li><li>• Decrypt - Packets dropped during decryption processing errors.</li><li>• Invalid SPI - Packets dropped due to packets containing Invalid SPI numbers.</li><li>• Authentication - Packets dropped due to authentication errors.</li><li>• Areplay - Packets dropped due to the anti-replay errors.</li></ul>
Last Statistics Reset	<p>Identifies the time that the channel stats were reset by a CTP or SNMP Manager command.</p>

**Possible Channel State Strings**

This table describes the possible Channel States that can be displayed in Figure 3-15.

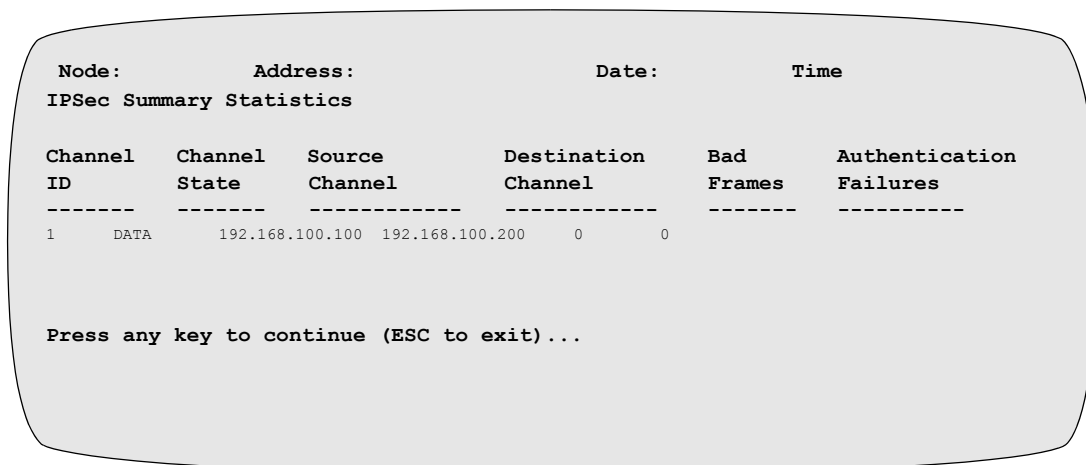
<b>Channel State</b>	<b>Indicates</b>
INIT	Trying to establish ISAKMP SA with remote.
ISAKMP	Successfully negotiated ISAKMP SA with remote peer.
DATA	Successfully established ESP and AH with remote peer, user data passing is enabled.
NON-DATA	Has established ISAKMP SA with remote, but has not yet established ESP or AH with the remote peer.

**IPSec All Channel Statistics**

This menu selection shows IPSec Statistics for all the channels, page by page, that have been configured and are currently active. Pressing “any key to continue” at the statistics screen will show the screen of the next active channel (if it exists).

**IPSec Summary Statistics**

Figure 3-16 shows the IPSec Summary Statistics.



**Figure 3-16. IPSec Summary Statistics**

**Screen Terms**

Below are the screen terms for the IPSec Summary Statistics:

<b>Screen Term</b>	<b>Description</b>
Channel ID	A number that uniquely identifies the IPSec channel.
Channel State	Identifies the activity state of the channel for each direction. <ul style="list-style-type: none"> <li>• Data: Indicates that normal data is passing through the channel.</li> <li>• No Data: Indicates that a channel is blocked for data traffic.</li> </ul>
Source Channel	Identifies the Source's IP Address
Destination Channel	Identifies the Destination's IP Address
Bad Frames	Number of packets that are dropped during the IPSec encryption process. This may be due to ESP/AH authentication failures for example.
Authentication Failures	Number of key exchange failures during the ISAKMP negotiations in both Phase 1 and Phase 2.

## SNMP IPsec Statistics

### Introduction

The IPsec statistics are made available via the cdx6500IPsecStatTable, which is indexed by the channel number cdx6500IPsecChanNum.

<b>MIB Table Name</b> cdx6500IPsecStatTable
<b>MIB Entry Name</b> cdx6500IPsecStatTableEntry
<b>Index(s)</b> IPsecStatChanNum
<b>OID Tree Location</b> .iso.org.dod.internet.private.enterprises.codex.cdxProductSpecific.cdx6500.cdx6500Statistics.cdx6500StatOtherStatsGroup.cdx6500IPsecStatTable.cdx6500IPsecStatTableEntry.IPsecStatChanNum

The table below indicates the names of the MIB Variables, their access attributes, correspondence to the relevant IPsec statistics and the display type. The description of each object as defined in the MIB should be the same as the help text associated with the CTP statistic variable.

### Contents of cdx6500IPsecStatTableEntry

<b>Object Name</b>	<b>Access Attributes</b>	<b>IPsec Statistic</b>	<b>Type</b>
IPsecStatChanNum	Read Only	Channel Number (index)	Integer
IPsecStatChanState	Read Only	Channel State	Display String
IPsecStatSrcChan	Read Only	Source Channel	IP Address
IPsecStatDestChan	Read Only	Destination Channel	IP Address
IPsecStatProfName	Read Only	IPsec Profile Name	Display String
IPsecStatPresharedKey	Read Only	Preshared Key <xxxx>	Display String
IPsecStatNegISAKMPProtect	Read Only	Negotiated ISAKMP Protection	Display String
IPsecStatAHProtect	Read Only	AH Protection	Display String
IPsecStatESPProtect	Read Only	ESP Protection	Display String
IPsecStatSATimeLimit	Read Only	SA TimeLimit (min)	Integer
IPsecStatSACharCountCurr	Read Only	SA Char Count (KBytes) (curr)	Integer
IPsecStatSACharCountLimit	Read Only	SA Char Count (KBytes) (limit)	Integer
IPsecStatISAKMPIPSEC Failures	Read Only	ISAKMP / IPSEC Failures	Counter
IPsecStatPktsPrbsdSent	Read Only	Packets Processed (Sent)	Counter
IPsecStatPktsPrbsdRcvd	Read Only	Packets Processed (Received)	Counter

**Contents of cdx6500IPSecStatTableEntry (continued)**

<b>Object Name</b>	<b>Access Attributes</b>	<b>IPSec Statistic</b>	<b>Type</b>
IPSecStatPktsDrpdNDState	Read Only	Packets Dropped (ND State)	Counter
IPSecStatPktsDrpdInvalidSPI	Read Only	Packets Dropped (Invalid SPI)	Counter
IPSecStatPktsDrpdFailedInteg	Read Only	Packets Dropped (Failed Integ)	Counter
IPSecStatLastStatisticReset	Read Only	Last Statistics Reset	Display String
IPSecStatBadFrames	Read Only	Bad Frames	Counter
IPSecStatAuthFailures	Read Only	Authentication Failures	Counter
IPSecStatBytesEncr	Read Only	Number of bytes Encrypted	Counter
IPSecStatBytesDecr	Read Only	Number of bytes Decrypted	Counter
IPSecStatDrpdEncr	Read Only	Packets Dropped (Encryption processing errors)	Counter
IPSecStatDrpdDecr	Read Only	Packets Dropped (Decryption processing errors)	Counter
IPSecStatDrpdEncrAuth	Read Only	Packets Dropped (Authentication errors during encryption processing)	Counter
IPSecStatDrpdDecrAuth	Read Only	Packets Dropped (Authentication errors during decryption processing)	Counter
IPSecStatDrpdReplay	Read Only	Packets Dropped (Due to anit replay errors)	Counter
IPSecStatISAKMPNegFail	Read Only	ISAKMP Phase 1 Negotiation Failures	Counter
IPSecStatIPSECNegFail	Read Only	ISAKMP Phase 2 Negotiation Failures	Counter
IPSecStatIPSECRejProposal	Read Only	Number of Rejected IPSec Proposals	Counter
IPSecStatIPSECInvdProposal	Read Only	Number of Invalid IPSec Proposals	Counter
IPSecStatIKSAMPDecrFail	Read Only	Number of Decryption Failures during ISAKMP Packet Processing	Counter
IPSecStatIKSAMPHashFail	Read Only	Number of hash failures during ISAKMP Packet Processing	Counter
IPSecStatSrcProxyAddr	Read Only	Source Proxy Address	IP Address
IPSecStatSrcProxyMask	Read Only	Source Proxy Mask	IP Address
IPSecStatDstProxyAddr	Read Only	Destination Proxy Address	IP Address
IPSecStatDstProxyMask	Read Only	Destination Proxy Mask	IP Address

# Chapter 4

## Digital Certificates and SCEP

---

### Overview

#### Introduction

---

This chapter provides a detailed description of X.509 Digital Certificate and Simple Certificate Enrollment Protocol (SCEP) features:

- X.509 Digital Certificate
- (SCEP) Enrollment
  - (SCEP) Support for IP Security (IPSec)

The SCEP and Digital Certificate feature is available in the Vanguard 340 Enhanced, 342 and 7300 Series products using release 6.4 and greater software. The Vanguard 340 Enhanced and 342 support the ECC DIM. The Advanced Encryption Card (AEC) is used on the 7300 Series.

#### ■ Note

Digital Certificates are used to authenticate Vanguard router-to-router sessions or sessions with IPSec compliant devices. Digital Certificate and SCEP are supported on the IPSec application only.

---

## X.509 Digital Certificate

---

### Introduction

The ITU-T standard X.509 defines a common format for certificates. This includes the type of information that might be present in a certificate and the rules for processing this information when validating certificates. X.509 uses Abstract Syntax Notation 1 (ASN.1) notation to describe certificates and the ASN.1 Distinguished Encoding Rules (DER) to encode objects for sending.

There are three versions of X.509 certificates, the main difference between these being the addition of unique identifier fields in v2 and the addition of arbitrary certificate extensions in v3. These extensions help extend the semantics of the certificate without the need to constantly redefine the syntax

Names of Certificate Authority's (CAs) and certificate subjects are specified in X.509 using an X.501 distinguished name. A distinguished name is simply a set of attribute and value pairs that uniquely identify a person or entity. Distinguished names were originally created to identify entries in an X.500 directory (X.509 certificates were created primarily to provide authentication for X.500 directories) and are also used in the same way in the Lightweight Directory Access Protocol (LDAP).

X.509 digital certificate can contain as many as eleven different fields, as shown in Figure 4-1. The most significant fields include:

- Subject - which identifies the entity that owns the private key
- Subjects Public Key - which is the public key of the subject
- Issuer
- Signature - Issuers Signature
- Period of Validity - Certificate validate time.

Version
Serial Number
Signature
Issuer
Period of Validity
Subject
Subject's Public Key
Issuer Unique ID
Subject Unique ID
Extensions
Encrypted

**Figure 4-1. X.509 Digital Certificate (Eleven Fields)**

## Certificate Management

To obtain a certificate, an entity must first register or enroll with a Certificate Authority (CA). This process establishes the user's authentication credentials and establishes a binding between that user and their public key. A CA usually requires Proof-Of-Possession (POP) of the private key. This is accomplished by the user creating a digital signature on the document and validating this document using their supplied public key. Once the CA has authenticated the user's details and performed POP, they generate the certificate and may publish it in an HTTP or LDAP repository.

One of the trust structure used in PKI context is hierarchy trust architecture, the trust structure starts from a root CA (which has a root certificate), which may issue subordinate trusted certificates, which can still issue even lower level subordinate certificates, and finally identity certificates are issued for specific system, host or even a person. If a root CA is trusted, all the subordinate certificates and identity certificates are trusted.

## Simple Certificate Enrollment Program (SCEP)

### Introduction

---

The Simple Certificate Enrollment Program (SCEP) protocol was developed by Cisco Systems and Verisign Incorporated to automate certificate enrollment for devices such as routers. It uses a PKCS#10 request which is in turn encrypted and sent to the CA along with transaction information. The CA either automatically approves the request and returns a certificate, or it returns a pending message and the device can return later to check if its request has been fulfilled.

SCEP encrypts the request to avoid revealing potentially sensitive information such as the IP addresses of devices which are using Network Address Translation (NAT) behind a firewall.

In addition to providing a mechanism for certificate enrollment, SCEP allows the device to obtain CA certificates and certificate paths.

The goal of SCEP:

- CA and RA public key distribution
- Certificate enrollment
- Certificate revocation
- Certificate query
- CRL query

SCEP makes use of existing technology for certificate enrollment, as listed below:

- Certification request format: PKCS #10
- Digital envelope syntax (message protocol): PKCS #7
- Transport protocol: HTTP
- Certificate format: X509.V3
- Public key algorithm: RSA only

### PKCS#10 Certificate Request

---

The PKCS#10 Certificate Request format was created to provide an online mechanism for requesting certificates. A PKCS#10 request contains the user's public key and a list of fields the user enters into the certificate. The request is then digitally signed with the user's private key. The CA can examine the request, use the contained public key to verify the request (effectively performing POP) and copy the fields from the PKCS#10 to the certificate (possibly adding, deleting or modifying information according to their local policy). PKCS#10 also provides a means to add a challenge password to the request, which can be used by the CA to authenticate the user. Alternatively, the CA may choose some other out-of-band mechanism for authentication.

Typically a user generates a PKCS#10 request which is encoded in a text format and then cut and paste this request into a standard HTML form to request the certificate. However, the PKCS#10 request can also be used by more sophisticated protocols such as SCEP to fully automate the enrollment process.

**PKCS#7  
Cryptographic  
Message Syntax  
Standard**

---

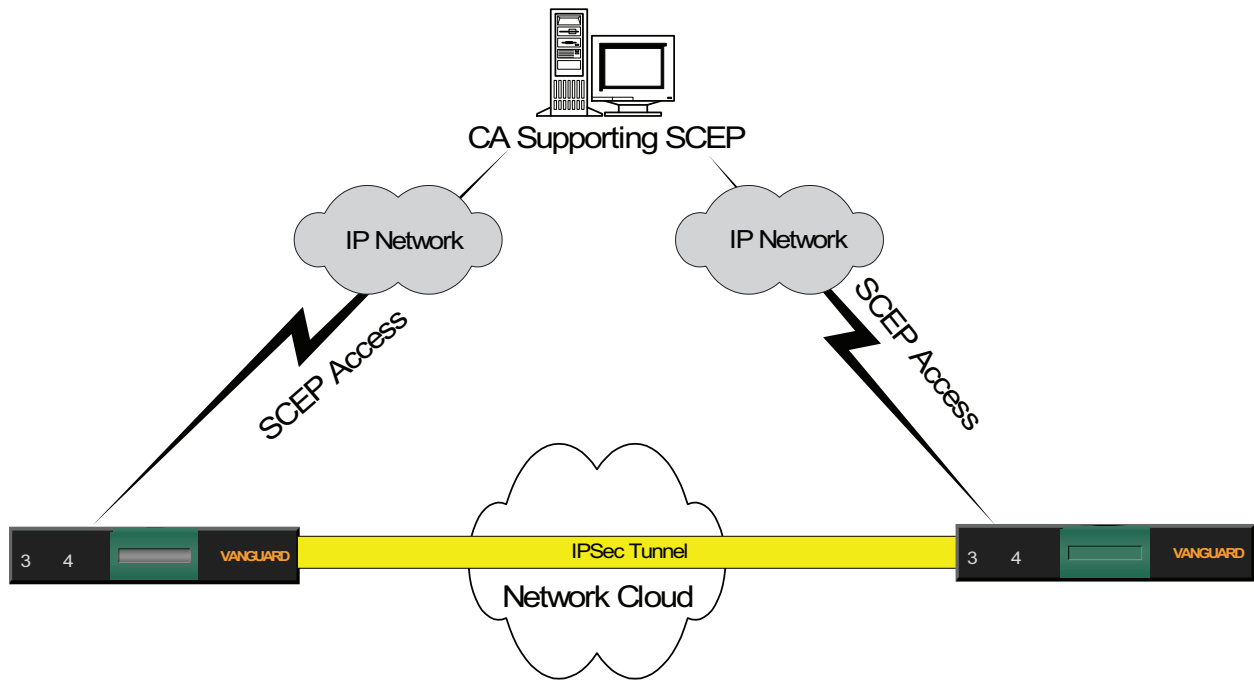
PKCS#7 defines a general syntax for data that may have cryptography applied to it, such as digital signatures and digital envelopes, it allows arbitrary attributes, such as signing time, to be authenticated along with the content of a message, and provides for other attributes such as counter signatures to be associated with a signature. This syntax is used in SCEP protocol to package and envelope messages to be exchanged between client and server.

---

## Applications and Solutions Support

### IPSec

Figure 4-2 shows the support ISAKMP protocol for digital certificate-based authentication to setup Security Association (SA).



**Figure 4-2. IPSec and SCEP**

### Secure Sockets Layer (SSL)

Digital certificate used for embedded web server.

■ **Note**

Release 6.4 and greater supports Digital Certificate and SCEP in the IPSec application only.

## Detailed Functional Description

### Digital Certificate Function (X.509 V3)

X.509 Certificate functions provide lower level service supporting key and certificate manipulation, encoding/decoding, signing and verification, etc., these functions are the basics for higher level public key functions such as key management protocols such as SCEP and public key applications such as IPSec and Secure Sockets Layer (SSL).

The following tasks are performed to obtain, install and manage certificates:

- Obtain and install one or more CA certificate(s)
- Enroll with the CA (whose certificate was installed in previous task)
  - Generate certificate request for one or more identity certificate(s)
- Certificate management, including List/View/Delete certificates

The following sections describe these functions respectively.

### Obtain and Install One or More CA Certificate(s)

Before any identity certificate can be enrolled with a CA, the CA's certificate must be first configured and then installed in the same node. SCEP protocol is used for online installation of CA certificate.

Release 6. 4 and greater supports SCEP servers including Microsoft Certificate Server and Verisign Onsite.

Reference “Install CA Certificates with SCEP” section on page 4-14 for CA certificate configuration and “HTTP” section on page 4-24 for certificate installation.

#### ■Note

To ensure the authenticity of the root certificate, the router administrator is expected to compare the root certificate fingerprint with the image in the server administrator. The fingerprint of the root certificate is an MD5 hash of the complete root certificate.

### Enroll Identity Certificate with the CA

In this operation, the device exchanges SCEP messages with the CA in order to enroll a ID certificate for the device.

Private key and public key will be generated first, the private key is stored in the local storage and is not visible to user, the public key will be packaged into a certificate require to be sent to the CA.

The certificate key size can be 512, 768, 1024 and 2048 bits.

Currently the SCEP protocol only support RSA key digital certificate.

The possible results of this operation are:

- 1) Cannot setup connection with CA, an alarm is generated.
- 2) The CA does not issue the certificate immediately base on its policy, the certificate request enters polling mode. By default, the node re-sends the request every 5 minutes for 15 times, after that, the time out error message is generated.
- 3) The CA reject the request, alarm with error message is generated
- 4) The CA approves the request and sends back a identity certificate to the node.

A message is displayed for successfully receiving the ID certificate.

Reference “Identity Certificate Enrollment with SCEP” section on page 4-14 for more information.

---

### Certificate Management

Certificate Management includes Certificate List/View/Delete certificate and certificate requests. Reference “Certificate Management” section on page 4-18 for Certificate List, View and Delete information.

- 1) The certificates are installed from top to bottom, and they must be deleted from bottom to top. The identity certificates must be deleted first, then delete any subordinate CA/RA certificate, and finally delete the root CA certificate. Otherwise, an error message is displayed and the operation is rejected.
- 2) To delete an identity certificate, usually the certificate should be revoked also. The revocation procedure defined in SCEP is a manual process. In order to revoke a certificate, the device administrator makes a phone call to the CA server operator, the operator asks for the Challenge Password (which has been sent to the server in the certificate request). If the Challenge Password matches, the certificate is revoked. This indicates that the user must write down the Challenge Password manually when enrolling an ID certificate. The node will not keep this information for security reasons.

---

### Certificate Storage

The certificate storage is a secure file system, it stores CA certificates and identity certificates as well as public key and private key. It stores maximum of twenty certificates (including CA/RA identity certificates).

Private key is stored together with the ID certificate that owns it, and it is encrypted and is not accessible to the user.

---

### Certificate ID

The ID certificates used in the node supports Domain Name (DN) (subject name), the IP address and Fully Qualified Domain Name (FQDN) (a subject alternative name). This indicates that the information will be embedded into the certificate.

The Vanguard device internal IP address can be used as the IP address, Vanguard device node name is recommended to be used as the FQDN.

#### ■ Note

If the internal IP address is used, this will indicate that the certificate for the node is issued and the internal IP address cannot be changed.

---

### Certificate Timing

Digital certificates are time-sensitive. Before applying for or receiving any certificates, the system clock must be set to the right date and time or the network timing protocols (such as SNTP) must be configured, working properly and synchronized with network time. Digital certificates indicate the time frame during which they are valid.

---

### Auto Renewal

Auto renewal is available with Release 6.4.S100 and greater software. When a digital certificate expires, the Vanguard unit automatically requests a new certificate from the CA. The auto renewal is only for expired certificates, not for revoked certificates. This feature is configurable. If it was not configured for a certificate, the system upon expiry would not request renewal. For a revoked certificate the user has to contact the CA and get a new certificate manually.

---

**Certificate  
Revocation List  
(CRL)**

Release 6.4.S100 and greater supports Certificate Revocation List. The SCEP client obtains the CRL from a distribution point (DP) via HTTP. The distribution point should be configured by the user under the CA configuration menu and the user should get the CRL manually the first time. After that the system updates the CRL automatically.

---

**IPSec with Digital  
Certificate  
Function**

Before an IPSec connection can be established between two nodes, each node must authenticate its peer. This authentication can be performed with the use of digital certificates. Each node sends its ID certificate, and a digital signature. The nodes must then validate the certificate sent by the peer and verify the signature. If the certificate or signature is invalid, the IPSec connection is terminated. This entire process is performed with the use of the Internet Key Exchange (IKE) protocol.

---

**Product Packaging**

Two software modules are created:

- **cert** - for digital certificate
- **scep** - for SCEP
  - **cfile** - for file system supporting certificate store

■ **Note**

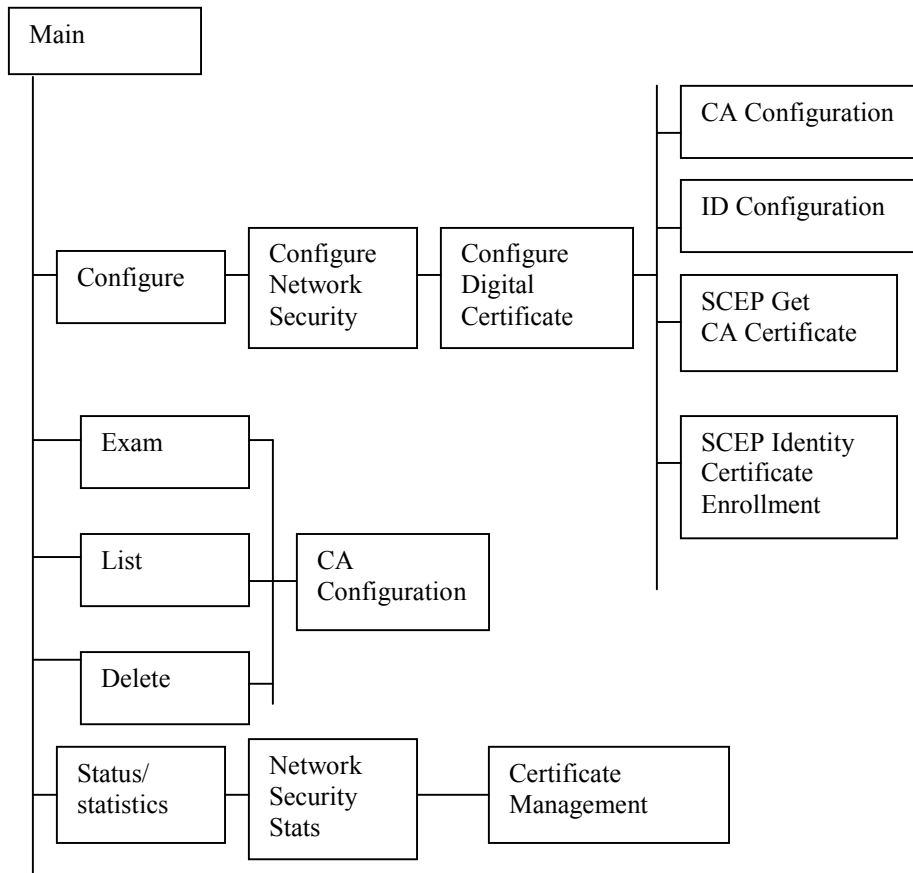
The modules cert, scep and cfile are linkable options.

---

## Configuration Menu

### Digital Certificate and SCEP Menu

Figure 4-3 shows the Digital Certificate and SCEP menu:



**Figure 4-3. SCEP and Digital Certificate CTP Menu**

## Configuration

**CA Configuration** Follow these steps to access Configure Digital Certificate from the Network Security Menu:

<b>Step</b>	<b>Action</b>	<b>Result</b>
<b>1</b>	Select <b>Configure</b> , from the CTP Main menu.	The Configure menu appears.
<b>2</b>	Select <b>Configure Network Security</b> .	The Configure Network Security Menu is shown.
<b>3</b>	Select <b>Configure Digital Certificate</b> .	

```

Node: v342-1      Address: (blank)      Date: 12-APR-2004  Time:
15:02:09
Menu: Configure Network Security      Path: (Main.6.18)

1.  Configure Encryption
2.  Configure IPSec
3.  Configure Digital Certificate

```

**Figure 4-4. Configure Network Security**

The following Certificate Authority (CA) configuration parameters are listed below:

**Main Menu->Configure->Configure Network Security->Configure Digital Certificate->CA Configuration**

### CA Name

Range:	1 to 8 (Character String)
Default:	(Blank)
Description:	This is the Certificate Authority (CA) name used internally in the software system and is not shown in the certificate. It is similar to a file name in the file system, it is used to index and identify a certificate inside the software system. The name for a certificate must not be the same as another one in the same node.

### CA URL

Range:	A string length less than 100 characters
Default:	(Blank)
Description:	The CA's URL (for example http://10.10.10.1:8080/abdc/efgh.cgi) for CA certificate installation and identity certificate enrollment. The format is HTTP:// followed by the IP address or DNS name of the CA. If the port number is something other than 80, include it after the IP address or DNS name separated with a colon(:). Following is the CA CGI path information for the SCEP Server Function.

### CA Descriptor

Range:	A string less than 64 characters
Default:	(Blank)
Description:	Some CAs use descriptors to further identify the certificate, in this case, the descriptor given by the CA should be entered here, otherwise, ignore this parameter. Currently, Verisign onsite request this field to match the registered domain name.

### Polling Interval

Range:	1 to 60
Default:	5
Description:	This Parameter is used for CA Certificate. If the CA does not issue the certificate immediately (some CAs require manual verification of credentials), the certificate request will enter polling mode. This parameter specifies the time period between certificate request re-sends for all identity certificate enrolled with this CA

**Polling Limit**

Range:	0 to 64
Default:	15
Description:	This parameter is used for CA certificate, and used together with the Polling Interval parameter. Specifies the number of times the node should re-send the certificate request when it does not receive a response from the previous request. Value of 0 means no re-send required.

**Operation  
Procedure: CA  
Certificate  
Configuration**

CA certificate configuration provides enough information to start installing a CA certificate.

The parameters to be configured are:

- CA Name
- CA URL
- CA Descriptor
- Certificate Enrollment Polling Interval
- Certificate Enrollment Polling Limit

**Entry Number: 1/**

[1] Certificate Authority Name: (blank)/ca1  
 [1] SCEP URL: (blank)/http://150.83.217.20:8080/scep.cgi  
 [1] CA Descriptor: (blank)/vgca1.com  
 [1] Certificate Enrollment Polling Interval:5/1  
 [1] Certificate Enrollment Polling Limit:15/;

**Install CA  
Certificates with  
SCEP**

The following Install Certificate Authority (CA) Certificates with SCEP information is shown in Figure 4-5:

**Main Menu->Configure->Configure Network Security->Configure Digital Certificate->SCEP Get CA Certificate**

```
Node: Nodename Address: (blank) Date: 5-FEB-2004 Time: 13:20:30
Menu: Configure Digital Certificate Path: (Main.6.18.3)

1. CA Configuration
2. ID Configuration
3. SCEP Get CA Certificate
4. SCEP Enroll ID Certificate

#Enter Selection: 3

SCEP Get CA Certificate

List of Configured CAs

1 - MSCA1
2 - LINUXCA
3 - VERISIGN

Enter CA number (1 - 3): 1
Connecting to the server, please wait...

CA certificate fingerprint computed:
0c:10:50:df:a1:d7:e2:4b:13:85:ff:3e:56:bc:0b:94

Do You Accept This Certificate (y/n): y

Certificate Saved.
```

**Figure 4-5. Installs CA Certificates through SCEP Online Protocol**

**Identity Certificate  
Enrollment with  
SCEP**

The following Identity Certificate Enrollment with SCEP information is below:

**Main Menu->Configure->Configure Network Security->Configure Digital Certificate->SCEP Enroll ID Certificate**

This menu enrolls identity certificate with a CA whose certificate already installed in previous steps.

Node: Nodename Address: (blank) Date: 5-FEB-2004 Time: 13:29:23  
Menu: Configure Digital Certificate Path: (Main.6.18.3)

1. CA Configuration
2. ID Configuration
3. SCEP Get CA Certificate
4. SCEP Enroll ID Certificate

#Enter Selection: 4  
SCEP Enroll ID Certificate  
List of Configured Cas

- 1 - MSCA1
- 2 - LINUXCA
- 3 - VERISIGN

Enter CA number (1 - 3): 1  
ID Certificate Name: VG1/  
Fully Qualified Domain Name (FQDN): fqdn.vg/  
IP Address: 150.83.217.102/  
Common Name (CN): VG\_CN/vg1\_cn  
Organization (O): Vanguard Networks/  
Organization Unit (OU): App\_Node/  
Country (C): CA/  
Public Key Size: 512 bits/  
Challenge Password: \*\*\*\*\*/.....  
Verify Challenge Password: \*\*\*\*\*/.....  
Send VG1 ID certificate request to CA MSCA1.(Y/N): y  
VG1: Generating key pair...  
VG1: Building certificate request message...  
VG1: Connecting to CA server...  
VG1: ID certificate request sent to CA.  
VG1: Certificate received and saved successfully

**Figure 4-6. Enrolls Identity Certificate with a CA**

**Fields in a Certificate Request**

The table below explains the meaning of each field:

<b>Field Name</b>	<b>Content</b>
Common Name (CN)	The primary identity of the entity associated with the certificate, for example, router 1. You must enter a name in this field.
Organizational Unit (OU)	The name of the department or other organizational unit to which this device belongs, for example: ABCD
Organization (O)	The name of the company or organization to which this device belongs, for example: Vanguard Managed Solution.
Subject Alternative Name, Fully Qualified Domain Name (FQDN)	The fully qualified domain name that identifies this device in this PKI, for example: router1.Vanguard Networks.com.  This field is optional. The alternative name is an additional data field in the certificate that provides interoperability with many other vendor products such as Cisco IOS and PIX systems in LAN-to-LAN connections.
Challenge Password	This field is optional, use this field according to the policy of your CA: <ul style="list-style-type: none"> <li>• Your CA might have given you a password. If so, enter it here for authentication.</li> <li>• Your CA might allow you to provide your own password to identify yourself to the CA in the future. If so, create your password here.</li> <li>• Your CA might not require a password. If not, leave this field blank.</li> </ul>
Verify Challenge Password	Re-enter the password for verification.

<b>Field Name</b>	<b>Content</b>
Key Size	<p>The algorithm for generating the public-key/private-key pair, and the key size. For requesting an identity certificate using SCEP, only the RSA options are available.</p> <ul style="list-style-type: none"><li>• RSA 512 bits = Generate 512-bit keys using the RSA (Rivest, Shamir, Adelman) algorithm. This key size provides sufficient security and is the default selection. It is the most common, and requires the least processing.</li><li>• RSA 768 bits = Generate 768-bit keys using the RSA algorithm. This key size provides normal security. It requires approximately 2 to 4 times more processing than the 512-bit key.</li><li>• RSA 1024 bits = Generate 1024-bit keys using the RSA algorithm. This key size provides high security, and it requires approximately 4 to 8 times more processing than the 512-bit key.</li><li>• RSA 2048 = Generate 2048-bit keys using the RSA algorithm. This key size provides very high security. It requires 8 to 16 times more processing than the 512-bit key.</li><li>• DSA 512 bits = Generate 512-bit keys using DSA (Digital Signature Algorithm).</li><li>• DSA 768 bits = Generate 768-bit keys using the DSA algorithm.</li><li>• DSA 1024 bits = Generate 1024-bit keys using the DSA algorithm.</li></ul>

---

## Certificate Management

### Certificate Management

Certificate Management can be accessed from the Control Terminal Ports (CTP) Main Menu:

**Main Menu->Status/statistics->Network Security Stats->Digital Certificate Stats->Certificate Management**

This menu lists, views and deletes existing certificates and/or certificate requests, but it does not change or delete the CA configuration

Operation Procedures:

- Certificate List
- Certificate View
- Certificate Delete

```

Node: Nodename Address: (blank) Date: 5-FEB-2004 Time: 14:03:24
Menu: Digital Certificate Stats Path: (Main.5.18.3)

1. Certificate Management

#Enter Selection: 1

Certificate Management

Entry Name Type Parent
=====
1 MSCA1 CA
2 VG1 ID MSCA1
3 MSCA1 RA
4 MSCA1 RA
5 VG2 ID Req MSCA1
6 LINUXCA CA

Press 'V' to View certificate,'D' to Delete certificate:
    
```

**Figure 4-7. Certificate List**

Certificate Management			
Entry	Name	Type	Parent
1	MSCA1	CA	
2	VG1	ID	MSCA1
3	MSCA1	RA	
4	MSCA1	RA	
5	VG2	ID Req	MSCA1
6	LINUXCA	CA	

Press 'V' to View certificate,'D' to Delete certificate: (Press 'V')

View Certificate Entry No.(1 to 6): 2

Version: 3 (0x2)

Serial Number:  
13:cf:10:3b:00:00:00:01:62

Signature Algorithm: sha1WithRSAEncryption

Validity: From Feb 5 18:16:27 2004 GMT to Feb 5 18:26:27 2005 GMT

Issuer:  
emailAddress=l009@vanguardms.com/countryName=CA/stateOrProvinceName=Ontario/localityName=Mississauga/organizationName=VanguardMS/

Subject:  
unstructuredAddress=150.83.217.102/unstructuredName=fqdn.vg/countryName=CA/organizationName=Vanguardms/organizationalUnitName=App\_No

Public Key Algorithm:rsaEncryption

Key Size: 512 bits

Modulus:  
c7:d0:1c:11:4f:7c:f3:4b:18:cf:d7:11:67:ad:57:1e

### Figure 4-8. Certificate View

An ID request has three valid states:

- 1) Pending state: in this state an ID request has been sent to CA and awaits the ID certificate issuing by CA. In the view of an ID request in pending state, number of CA polling will be displayed.
- 2) Pending Done: in this state the system polled the CA the number of times configured in CA configuration and CA had not responded by issuing an ID certificate.

- 3) Failure: in this state the ID request was failed and no certificate has been issued or the issued certificate was invalid. During the view of such ID request the cause of the failure will be displayed.

```
Node: Nodename Address: (blank) Date: 5-FEB-2004 Time: 14:30:26
Menu: Digital Certificate Stats Path: (Main.5.18.3)
1. Certificate Management
#Enter Selection: 1
Certificate Management

Entry Name Type Parent
=====
1 M S C A 1 CA
2 V G 1 ID M S C A 1
3 M S C A 1 RA
4 M S C A 1 RA
5 V G 2 ID Req M S C A 1
6 L I N U X C A CA
Press 'V' to View certificate, 'D' to Delete certificate: (Press "D")
Delete certificate Entry No.(1 to 6): 1
Number of ID certificate(s) issued by CA M S C A 1: 1.
Number of pending ID certificate request(s) for CA M S C A 1: 1.
Number of RA certificate(s) associated with CA M S C A 1: 2.

**** WARNING ****
Deleting a CA certificate causes the deletion of:
- all the ID certificates issued by the CA,
- all the ID certificate requests pending for the CA,
- all the RA certificates associated with the CA,
- the CA certificate.
The CA configuration remains in the system.
Do you want to delete CA M S C A 1 certificate?(Y/N): (Press 'Y')

ID certificate V G 1 deleted.
Please contact the CA to revoke the ID certificate.
```

Figure 4-9. Certificate Delete

## CA Configuration

**CA Configuration** Certificate Authority (CA) Configuration Records can be accessed to:

- Examine
- List
- Delete

Access these records from the Control Terminal Ports (CTP) Main Menu. The menus perform the regular examine/list/delete operation on the CA configuration records.

■ **Note**

To delete a CA configuration record, the associated CA certificate must be deleted first.

**Main Menu->Exam->Examine Network Security->Examine Digital Certificate->Examine CA Config**

```
Menu: Examine Digital Certificate      Path: (Main.2.18.3)
  1. Examine CA Config
  2. Examine default ID Config

#Enter Selection: 1

      CA Configuration Examination
Entry Number: 1/
[1] CA Name: ca1
[1] CA URL: http://150.83.16.4/certsrv/mscep/mscep.dll
[1] CA Descriptor: ca1
[1] Certificate Enrollment Polling Interval: 1
[1] Certificate Enrollment Polling Limit: 15

Entry Number: 2/
```

**Figure 4-10. Examine CA Configuration Record**

**Main Menu->List ->List Network Security->List Digital Certificate->List CA Config**

```
Menu: List Digital Certificate      Path: (Main.3.18.3)

  1. List CA Config
  2. List default ID Config
#Enter Selection: 1

      CA Configuration List

[1], ca1, http://150.83.16.4/certsrv/mscep/mscep.dll, ca1, 1, 15

[2], ca2, http://150.83.12.19/cgi-bin/pkiclient.exe, testca, 5, 15

[3], ca3, http://216.168.252.59/cgi-bin/pkiclient.exe, vgms.com, 1, 15

Press any key to continue ( ESC to exit ) ...
```

**Figure 4-11. List CA Configuration Record**

**Main Menu->Delete->Delete Network Security->Delete Digital Certificate->Delete CA Config**

```
Menu: Delete Digital Certificate    Path: (Main.10.18.4)

  1. Delete CA Config
  2. Delete default ID Config

#Enter Selection: 1

      Delete CA configuration record

Entry Number: 1/2

Proceed (y/n): y
      Record deleted.

Press any key to continue ( ESC to exit ) ...
```

**Figure 4-12. Delete CA Configuration Record**

## IPSec Configuration

### IPSec Configuration

IPSec can be configured to authenticate peers with RSA signatures via the ISAKMP Policy Table. Configuration parameters for RSA signatures are shown below. (Refer to Chapter Three of this manual for more detailed IPSec information.)

Figure 4-13 shows configurable parameters for the ISAKMP Policy table.

```

          Configure ISAKMP Policy Table
Entry Number: 1/
[1] Authentication Method: RSA_SIGNATURE/
[1] Diffie-Hellman MODP Group: 1/
[1] Encryption Algorithm: DES_CBC/
[1] Pseudo Random Function: MD5/
[1] ISAKMP Keepalive Idle Time: 30/
[1] ISAKMP Keepalive Retry Time: 10/
[1] ISAKMP SA Lifetime: 1440/

```

**Figure 4-13. ISAKMP Policy Table**

#### Authentication Method

Range:	PRE-SHARED_KEY, RSA_SIGNATURE
Default:	PRE-SHARED_KEY
Description:	The ISAKMP SA authentication method.
Boot Type:	Boot IPSec Policy Table

IPSec

IPSec Channel Statistics are shown in Figure 4-14.

```
Node: top      Address: (blank)      Date: 24-FEB-2003  Time: 12:02:07
Detailed IPSec Channel Statistics: Channel 1      Page: 1 of 1

Channel State:          DATA
Source Channel:         192.168.100.1 (Tnl no 1)
Destination Channel:   192.168.100.2
IPSec Profile Name:     profilename
Negotiated ISAKMP Protection:  DES, MD5, RSA-SIG, MODP 1, DPD

AH Protection:          MD5
ESP PROTECTION:         DES, MD5
SA Time Limit (Min):   385
SA Char Count (KBytes) (curr,limit): 5, 0
Anti-Replay Sliding Window Size: 32
Perfect Forward Secrecy: Enabled
ISAKMP / IPSEC Failures: 0
Packets Processed (sent, received): 48, 46
                                ND State   Invalid SPI   Failed Integ
Packets Dropped:       1           0           0
Last Statistics Reset: 24-FEB-2003 11:39:46

Press any key to continue ( ESC to exit ) ...
```

**Figure 4-14. Detailed IPSec Channel Statistics**

HTTP

Basic HTTP support has the same function as the CTP menu, automatically available after CTP menus are done.

## VPN Technical Glossary

---

### List of Acronyms:

AES	Advanced Encryption Standard
AH	Authentication Header
ASN.1	Abstract Syntax Notation One, as defined in X.208
BER	Basic Encoding Rules, as defined in X.209
CA	Certificate Authority
CRL	Certificate Revocation List
DCC	Data Compression Card
DER	Distinguished Encoding Rules for ASN.1, as defined in X.509
DES	Data Encryption Standards.
Diffie-Hellman	A key exchange mechanism developed by Martin Hellman, Bailey Diffie and Ralph Merkle. The patent of Diffie-Hellman key exchange algorithm (US Patent # 4,200,700) expired in April 29, 1997. DH key exchange algorithm is specified in IKE.
DOI	Domain of Interpretation
DSA	Digital Signature Algorithm. DSA is another public key system developed by NIST. DSA can be used for digital signature but cannot be used for encryption. There is no patent on this algorithm.
ECC	Encryption Compression Card
ECS	Encryption Control Subsystem
ESP	Encapsulated Security payload
FR	Frame Relay
GRE	Generic Routing Encapsulation
ICMP	Internet Control Message Protocol
IKE	Internet Key Exchange, renamed from Oakley key Exchanged protocol
IP	Internet Protocol
IPSEC	IP Security
ISAKMP	Internet Security Association Key Management Protocol
L2TP	Layer 2 Tunneling Protocol
LCON	Lan Connection

MD5	Message Digest 5
NAT	Network Address Translation
NIST	National Institute of Standards & Technology
OSPF	Open Shortest Path First
PEM	Privacy Enhanced Mail
PKCS	Public Key Cryptography Standards
PKI	Public Key Infrastructure
PKIX	X.509 based PKI
PFS	Perfect Forward Secrecy
PPP	Point to Point Protocol
RA	Registration Authority
RFC	Request For Comment
RIP	Routing Information Protocol
RSA	RSA refers to the public Key algorithm invented by Ron Rivest, Adi Shamir and Leonard Alderman, co-founders of the RSA (the company). RSA can be used for both encryption and digital signature. RSA's patent (US Patent # 4,405,829) expires on Sept 20, 2000.
SA	Security Association
SAD	Security Association Database
SAM	Security Association Management
SCEP	Simple Certificate Enrollment Protocol
SHA-1	Secure Hash Algorithm 1. Developed by the National Security Agency (NSA) or NIST. There is no patent on this algorithm.
SPD	Security Policy Database
SPI	Security Parameter Index
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
VPN	Virtual Private Network

**A**

Address on the Statistics Screen 2-17

**C**

CA Configuration 4-21  
Certification Revocation List (CRL) 4-9  
Configuration  
    Digital Certificate and SCEP 4-11  
Configuration Examples 2-32  
Configuration Menu  
    Digital Certificate and SCEP 4-10  
Configure Tunnel Table 2-12

**D**

Digital Certificate  
    Auto Renewal 4-8  
Digital Certificates and SCEP 4-1  
Dynamic Host Configuration Protocol (DHCP) 2-8  
Dynamic Tunnel Address 2-8  
Dynamic Tunnel Address Example with PPP over  
    WAN 2-13  
Dynamic Tunnel Address feature via DHCP 2-15  
Dynamic Tunnel Address feature via PPP over  
    Ethernet 2-14  
Dynamic Tunnel Address feature via PPP over  
    WAN 2-13  
Dynamic Tunnel Address Statistics 2-16

**G**

Generic Routing Encapsulation (GRE) 2-20  
GRE\_IPSec Example 3-19  
GRE\_IPSec Statistics 3-25

**I**

Internet 2-9  
Internet Security Association and Key Management  
    Protocol (ISAKMP) 2-9  
IP Control Protocol (IPCP) 2-8  
IP Security  
    3-1  
    Introduction 3-1  
    Vanguard IP Security 3-3  
IP Security (IPSec)  
    Configuration 3-5  
    Description 3-1  
    example 3-5  
    Implementation 3-3  
    Parameters 3-7  
    SNMP IPSec Statistics 3-31  
    Statistics 3-25  
IPSec Configuration 3-6  
IPSec Configuration Example 3-17

IPSec tunnels 2-8

**L**

Limitations 2-10

**P**

Point-to-Point Protocol (PPP) 2-8  
Point-to-Point Protocol over Ethernet (PPPoE) 2-8

**R**

Remote Node 2-12  
RTP/UDP/IP Header Compression of Tunneled  
    Packets 2-19

**S**

SCEP Applications and Solutions Support 4-6  
Simple Certificate Enrollment Program (SCEP) 4-4  
Statistics  
    GRE\_IPSec 3-25  
Statistics of Node with a Tunnel with a Dynamic  
    Source Address 2-17  
Statistics on Host Node 2-18  
Statistics on Remote Node 2-17  
Supported Platforms 2-10

**T**

Tunnel Application Sample 2-8  
Tunnel Boot 2-40  
Tunnel Encryption 1-5  
Tunnel Statistics 2-41  
Tunneling  
    Addresses 2-4  
    Configuration 2-24  
    Description 2-1  
    General Statistics 2-42  
    Outbound Operation 2-2  
    Overview 2-1  
    Parameters 2-24  
    Statistics 2-41

**V**

Virtual Private Network  
    Applications 1-3  
    Description 1-2  
VPN  
    Advantages 1-2  
    Introduction 1-1  
    Requirements 1-2  
VPN Tunneling 2-4  
    Examples 2-11  
VPN tunnels 2-8

## **X**

X.509 Detailed Functional Description [4-7](#)

X.509 Digital Certificate [4-2](#)

Management [4-3](#)

X.509 Digital Certificate

Function [4-7](#)