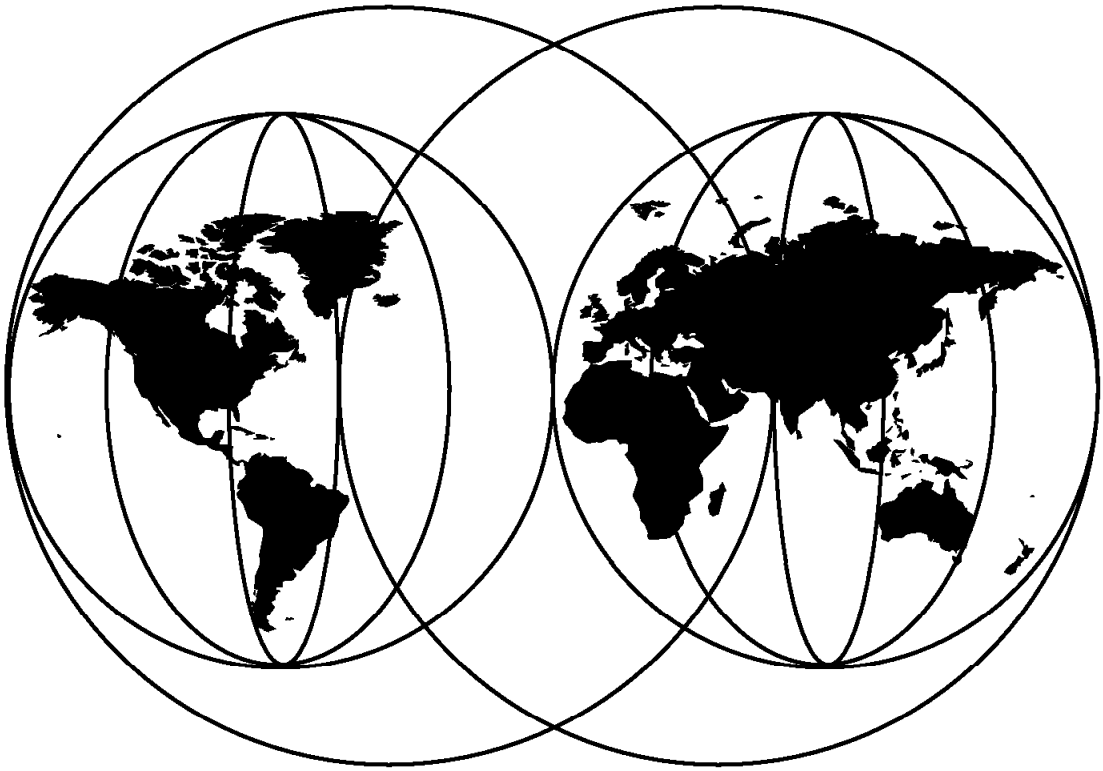
A Comprehensive Guide to Virtual Private Networks, Volume II: IBM Nways Router Solutions

Tim Kearby, Steven Boelaars, C. Steven Lingafelt, Kacir Samra



International Technical Support Organization

http://www.redbooks.ibm.com

SG24-5234-00

International Technical Support Organization

SG24-5234-00

A Comprehensive Guide to Virtual Private Networks, Volume II: IBM Nways Router Solutions

December 1998

Take Note!

Before using this information and the product it supports, be sure to read the general information in Appendix C, “Special Notices” on page 159.

First Edition (December 1998)

This edition applies to Nways Multiprotocol Routing Services (MRS), Nways Multiprotocol Access Services (MAS) Versions 3.1 and 3.2 for use with the IBM Nways 2210, 2212, and 2216 Multiprotocol Routers.

Comments may be addressed to:
IBM Corporation, International Technical Support Organization
Dept. HZ8 Building 678
P.O. Box 12195
Research Triangle Park, NC 27709-2195

When you send information to IBM, you grant IBM a non-exclusive right to use or distribute the information in any way it believes appropriate without incurring any obligation to you.

Contents

Preface

This redbook is Volume 2 in the series on Virtual Private Networks (VPNs). Whereas Volume I provides the reader with an understanding of the architecture and underlying technologies, this redbook is a practical guide for use in configuring IPSec tunnels and applications of these tunnels with IBM Nways Multiprotocol Routers.

The redbook is based on Versions 3.1 and 3.2 of Nways Multiprotocol Routing Services (MRS) and Nways Multiprotocol Access Services (MAS), which provide support for manually configured IPSec tunnels. It takes you step-by-step through the definition of a tunnel and the required packet filters that work together with IPSec to implement the architecture. Each parameter is fully explained in the context of using IBM 2210s and 2216s to create VPNs that link corporate enterprises to branch offices and business partners over the Internet and other untrusted networks.

The redbook delves further into these scenarios by showing you how to implement solutions that exploit Data Link Switching (DLSw), IP Bridging Tunnels, Enterprise Extender (HPR over IP), APPN DLUR, TN3270, and Layer 2 Tunneling Protocol (L2TP) through an IPSec tunnel.

A working knowledge of the IPSec protocols is assumed.

The Team That Wrote This Redbook

This redbook was produced by a team of specialists from around the world working at the International Technical Support Organization Raleigh Center.

Tim Kearby is an Advisory ITSO Specialist for Networking at the Systems Management and Networking ITSO Center, Raleigh. He writes redbooks and teaches workshops on local and wide area networking. Tim has held various positions in his IBM career including assignments in product development, systems engineering, and consulting. He holds a Bachelors of Science degree in Electrical Engineering from Purdue University.

Steven Boelaars is a Networking IT Specialist in IBM Global Services/Network Services in the Netherlands. His areas of expertise include TCP/IP and APPN, Frame-Relay networking and remote access. Steven has a Masters Degree in Applied Physics from the Delft University of Technology.

C. Steven Lingafelt is a Senior Engineer in IBM′s Networking Hardware Division in Research Triangle Park, NC. He has 16 years of experience in the networking field and is a Senior Member of IEEE. His areas of expertise include hardware architectures, multiprotocol routing, and IPSec based Virtual Private Networking. He has written extensively on many networking subjects for both internal IBM publications and external publications and holds numerous patents. He holds a BS in Electrical Engineering from Virginia Polytechnic Institute & State University and an MS in Telecommunications from Pace University.

Kacir Samra is a Systems Support Specialist, supporting the IBM Multiprotocol Network (MPN) in IBM Global Services, Brazil. He joined the company in 1993. He is a graduate of PUC University with a degree in Systems Analysis.

Thanks to the following people for their invaluable contributions to this project:

Martin Murhammer, Gail Christensen, Shawn Walsh,
Kathryn Casamento, Linda Robinson, Mike Haley
International Technical Support Organization, Raleigh Center

Garth Madella
IBM South Africa

Luke Gibbons
IBM Australia

Andreas Weinfurter
IBM Austria

Tamas Gaidosch
IBM Hungary

Lynda Linney
Installation Support Centre
IBM Hursley Park, U.K.

Cliff Wang
Ellen Cybrynski
Andy Arrowood
Jason Cornpropst
Don Grosser
Bruce Dillon
IBM NHD
Research Triangle Park, NC

Charles Kunzinger
Laura Rademacher
IBM NSD
Research Triangle Park, NC

Comments Welcome

Your comments are important to us!

We want our redbooks to be as helpful as possible. Please send us your comments about this or other redbooks in one of the following ways:

- Fax the evaluation form found in “ITSO Redbook Evaluation” on page 167 to the fax number shown on the form.
- Use the online evaluation form found at `http://www.redbooks.ibm.com/`
- Send your comments in an Internet note to `redbook@us.ibm.com`

Chapter 1. Introduction

Note

This chapter provides a brief introduction to Virtual Private Networks (VPNs) and the IETF framework for IP Security called IPSec. It is not meant to be a complete reference on the subject. For more information on the IPSec architectural framework, please see the companion redbook in this series entitled *A Comprehensive Guide to Virtual Private Networks, Volume I: IBM Firewall, Server and Client Solutions,* SG24-5201.

The Internet has become a popular, low-cost backbone infrastructure. Its universal reach has led many companies to consider constructing a secure virtual private network (VPN) over the public Internet. The challenge in designing a VPN for today's global business environment will be to exploit the public Internet backbone for both intra-company and inter-company communication while still providing the security of the traditional private, self-administered corporate network.

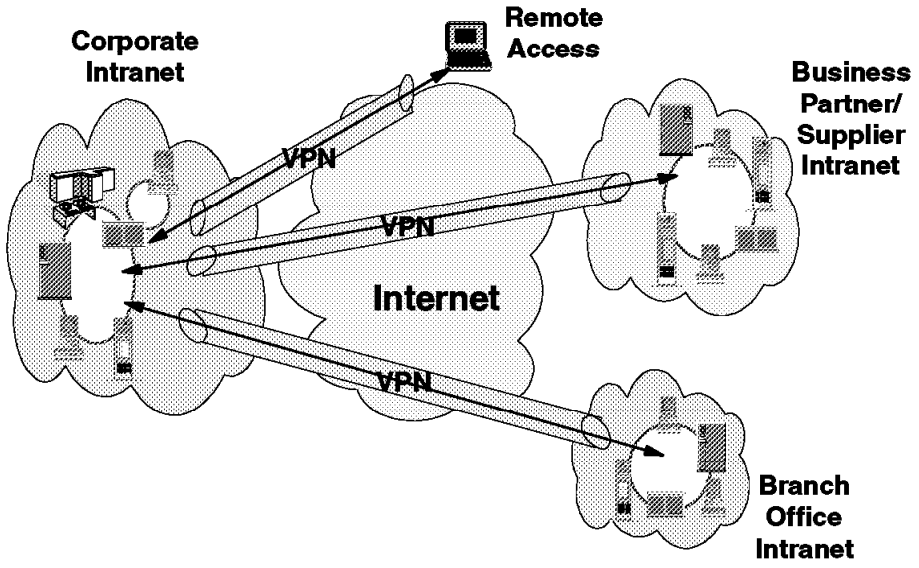


Figure 1. Virtual Private Networks

A virtual private network (VPN) is an extension of an enterprise's private intranet across a public network such as the Internet, creating a secure private connection, essentially through a private *tunnel*. VPNs securely convey information across the Internet connecting remote users, branch offices, and business partners into an extended corporate network, as shown in Figure 1. Internet Service Providers (ISPs) offer cost-effective access to the Internet (via direct lines or local telephone numbers), enabling companies to eliminate their current, expensive leased lines, long-distance calls, and toll-free telephone numbers.

1.1 The IETF′s IP Security Framework (IPSec)

Within the layered communications protocol stack model, the network layer (IP in the case of the TCP/IP stack) is the lowest layer that can provide end-to-end security. Network-layer security protocols provide blanket protection for all upper-layer application data carried in the payload of an IP datagram, without requiring a user to modify the applications.

The solutions are based on the IP Security Architecture (IPSec) open framework, defined by the IPSec Working Group of the IETF. IPSec is called a framework because it provides a stable, long lasting base for providing network layer security. It can accommodate today′s cryptographic algorithms, and can also accommodate newer, more powerful algorithms as they become available. IPv6 implementations are required to support IPSec, and IPv4 implementations are strongly recommended to do so. In addition to providing the base security functions for the Internet, IPSec furnishes flexible building blocks from which robust, secure virtual private networks can be constructed.

The IPSec Working Group has concentrated on defining protocols to address several major areas:

- *Data origin authentication* verifies that each datagram was originated by the claimed sender.
- *Data integrity* verifies that the contents of the datagram were not changed in transit, either deliberately or due to random errors.
- *Data confidentiality* conceals the cleartext of a message, typically by using encryption.
- *Replay protection* ensures that an attacker cannot intercept a datagram and play it back at some later time without being detected.
- *Automated management of cryptographic keys and security associations* ensures that a company′s VPN policy can be conveniently and accurately implemented throughout the extended network with little or no manual configuration. These functions make it possible for a VPN′s size to be scaled to whatever size a business requires.

The principal IPSec protocols are:

- IP Authentication Header (AH) provides data origin authentication, data integrity, and replay protection.
- IP Encapsulating Security Payload (ESP) provides data confidentiality, data origin authentication, data integrity, and replay protection.
- Internet Security Association and Key Management Protocol (ISAKMP) provides a method for automatically setting up security associations and managing their cryptographic keys.

1.1.1.1 Authentication Header (AH)

The IP Authentication Header provides connectionless (that is, per-packet) integrity and data origin authentication for IP datagrams, and also offers protection against replay. Data integrity is ensured by the checksum generated by a message authentication code (for example, MD5); data origin authentication is ensured by including a secret shared key in the data to be authenticated; and replay protection is provided by use of a sequence number field within the AH header. In the IPSec vocabulary, these three distinct functions are lumped together and simply referred to by the name *authentication*.

1.1.1.2 Encapsulating Security Payload (ESP)

The IP Encapsulating Security Payload provides data confidentiality (encryption), connectionless (that is per-packet) integrity, data origin authentication, and protection against replay. ESP always provides data confidentiality, and can also optionally provide data origin authentication, data integrity checking, and replay protection. Comparing ESP to AH, one sees that only ESP provides encryption, while either can provide authentication, integrity checking, and replay protection.

When ESP is used to provide authentication functions, it uses the same algorithms used by the AH protocol. However, the coverage is different.

1.1.1.3 Combining the Protocols

Either ESP or AH may be applied alone, in combination with the other, or even nested within another instance of itself. With these combinations, authentication and/or encryption can be provided between a pair of communicating hosts, between a pair of communicating firewalls, or between a host and a firewall.

1.1.1.4 ISAKMP/Oakley

A security association (SA) contains all the relevant information that communicating systems need in order to execute the IPSec protocols, such as AH or ESP. For example, a security association will identify the cryptographic algorithm to be used, the keying information, the identities of the participating parties, etc. ISAKMP defines a standardized framework to support negotiation of security associations (SA), initial generation of all cryptographic keys, and subsequent refresh of these keys. Oakley is the mandatory key management protocol that is required to be used within the ISAKMP framework. ISAKMP supports automated negotiation of security associations, and automated generation and refresh of cryptographic keys. The ability to perform these functions with little or no manual configuration of machines will be a critical element as a VPN grows in size.

Secure exchange of keys is the most critical factor in establishing a secure communications environment no matter how strong your authentication and encryption are, they are worthless if your key is compromised. Since the ISAKMP procedures deal with initializing the keys, they must be capable of running over links *where no security can be assumed to exist*. That is, they are used to *bootstrap* the IPSec protocols. Hence, the ISAKMP protocols use the most complex and processor-intensive operations in the IPSec protocol suite.

ISAKMP requires that all information exchanges must be both encrypted and authenticated. No one can eavesdrop on the keying material, and the keying material will be exchanged only among authenticated parties.

1.2 VPN Customer Scenarios

In this section we look at the three most likely business scenarios well suited to the implementation of a VPN solution:

1. Branch office connection network
2. Business partner/supplier network
3. Remote access network

This following sections provides a brief overview of each of these scenarios.

1.2.1 Branch Office Connection Network

The branch office scenario securely connects two trusted intranets within your organization. This is a key difference, since your security focus is on both protecting your company′s intranet against external intruders and securing your company′s data while it flows over the public Internet. This differs from the business partner/supplier network discussed in 1.2.2, “Business Partner/Supplier Network” on page 5, where the focus is on enabling your business partners/suppliers access to data in your corporate intranet.

For example, suppose corporate headquarters wants to minimize the costs incurred from communicating with its own branches. Today, the company may use frame relay and/or leased lines, but wants to explore other options for transmitting their internal confidential data that will be less expensive, more secure, and globally accessible. By exploiting the Internet, branch office connection VPNs can easily be established to meet the company′s needs.

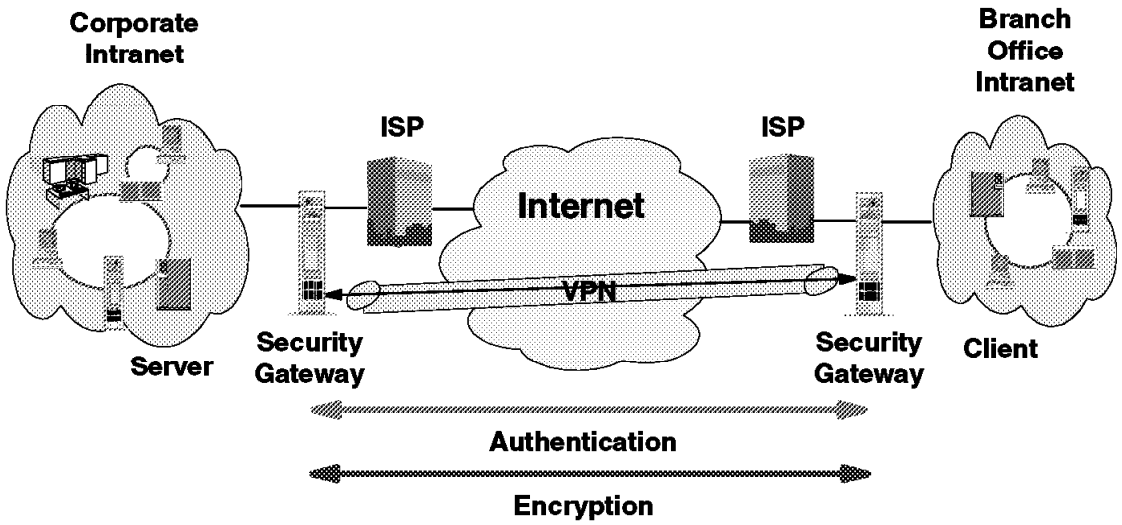


Figure 2. Branch Office Connection Network

As shown in Figure 2, one way to implement this VPN connection between the corporate headquarters and one of its branch offices is for the company to purchase Internet access from an ISP, such as IBM Global Services. IBM eNetwork firewalls, or routers with integrated firewall functionality, or in some cases an IBM server with IPSec capability, would be placed at the boundary of each of the intranets to protect the corporate traffic from Internet hackers. With this scenario, the clients and servers need not support IPSec technology, since the IPSec-enabled firewalls (or routers) would be providing the necessary data packet authentication and encryption. With this approach, any confidential information would be hidden from untrusted Internet users, with the firewall or router denying access to potential attackers.

With the establishment of branch office connection VPNs, the company′s corporate headquarters will be able to communicate securely and cost-effectively with its branches, whether located locally or far away. Through VPN technology, each branch can also extend the reach of its existing intranet to incorporate the other branch intranets, building an extended, enterprise-wide corporate network.

And, as in the business partner/supplier network scenario, this company can easily expand this newly created environment to include its business partners, suppliers, and remote users, through the use of open IPSec technology.

1.2.2 Business Partner/Supplier Network

Industry-leading companies will be those that can communicate inexpensively and securely to their business partners, subsidiaries, and vendors. Many companies have chosen to implement frame relay and/or purchase leased lines to achieve this interaction. But this is often expensive, and geographic reach may be limited. VPN technology offers an alternative for companies to build a private and cost-effective extended corporate network with worldwide coverage, exploiting the Internet or other public network.

Suppose you are a major parts supplier to a manufacturer. Since it is critical that you have the specific parts and quantities at the exact time required by the manufacturing firm, you always need to be aware of the manufacturer′s inventory status and production schedules. Perhaps you are handling this interaction manually today, and have found it to be time consuming, expensive and maybe even inaccurate. You′d like to find an easier, faster, and more effective way of communicating. However, given the confidentiality and time-sensitive nature of this information, the manufacturer does not want to publish this data on their corporate Web page or distribute this information monthly via an external report.

To solve these problems, the parts supplier and manufacturer can implement a VPN, as shown in Figure 3. A VPN can be built between a client workstation, in the parts supplier′s intranet, directly to the server residing in the manufacturer′s intranet. The clients can authenticate themselves either to the firewall or router protecting the manufacturer′s intranet, directly to the manufacturer′s server (validating that they are who they say they are), or to both, depending on your security policy. Then a tunnel could be established, encrypting all data packets from the client, through the Internet, to the required server.

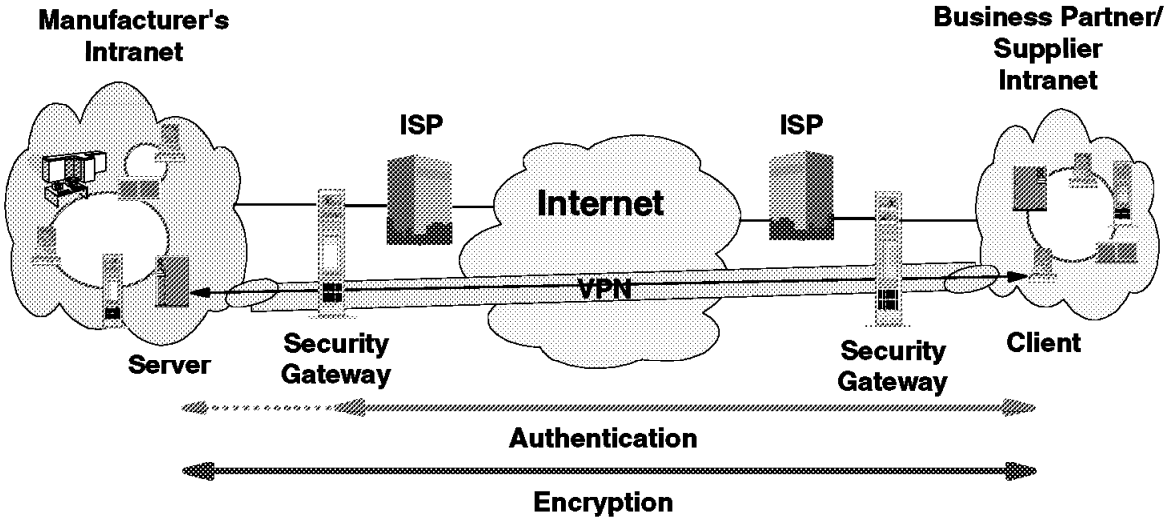


Figure 3. Business Partner/Supplier Network

With the establishment of this VPN, the parts supplier can have global, online access to the manufacturer′s inventory plans and production schedule at all times during the day or night, minimizing manual errors and eliminating the

need for additional resources for this communication. In addition, the manufacturer can be ensured that the data is securely and readily available to only the intended parts supplier(s).

One way to implement this scenario is for the companies to purchase Internet access from an Internet service provider (ISP), such as IBM Global Services. Then, given the lack of security of the Internet, either an IBM eNetwork firewall or IPSec-enabled router, or an IBM server with IPSec capability can be deployed as required to protect the intranets from intruders. If end-to-end protection is desired, then both the client and server machines need to be IPSec-enabled as well.

Through the implementation of this VPN technology, the manufacturer would easily be able to extend the reach of their existing corporate intranet to include one or more parts suppliers (essentially building an extended corporate network) while enjoying the cost-effective benefits of using the Internet as their backbone. And, with the flexibility of open IPSec technology, the ability for this manufacturer to incorporate more external suppliers is limitless.

Yet, inherent in network expansion are concerns of manageability. Tools should be implemented to ensure your network remains easy to maintain. Management functions to be included in future eNetwork VPN solutions are:

- Policy management
- Automated ISAKMP/Oakley key management capabilities
- Certificate management
- Secure domain name server (DNS)
- Lightweight Directory Access Protocol (LDAP) support

When implementing a VPN, a set of security configuration criteria must be established. Decisions such as which security algorithms are to be used by each IPSec-enabled box and when the keys are to be refreshed are all aspects of policy management. And, with respect to key technology, almost all of today′s currently popular security protocols begin by using public key cryptography. Each user is assigned a unique public key. Certificates, in the form of digital signatures, validate the authenticity of your identity and your encryption key. These certificates can be stored in a public key database, such as a secure DNS, that can be accessible via a simple protocol, such as LDAP.

An automated IP address management system is especially important for VPNs in order to assign and manage your network′s IP addresses. IBM is working with an IP address management company to offer highly centralized control of all network devices in your entire extended intranet. Also, along the lines of managing your IP addresses, network address translation (NAT), available today in several IBM products including the IBM Nways Multiprotocol Router family and the eNetwork Firewall for AIX, allows you to use a globally unique (public) address on the Internet, while enabling you to use private IP addresses within your intranet.

IBM will be incorporating all of these VPN management tools into its eNetwork VPN solutions, which can easily be implemented to meet the needs of your existing and future networking environment.

1.2.3 Remote Access Network

A remote user, whether at home or on the road, wants to be able to communicate securely and cost-effectively back to his/her corporate intranet. Although many still use expensive long-distance and toll-free telephone numbers, this cost can be greatly minimized by exploiting the Internet. For example, you are at home or on the road, but need a confidential file on a server within your intranet. By obtaining Internet access in the form of a dial-in connection to an ISP such as IBM Global Services, you can communicate with the server in your intranet and access the required file.

One way to implement this scenario is to use an eNetwork VPN IPSec-enabled remote client and firewall or router, as shown in Figure 4. The client accesses the Internet via dial-up to an ISP, and then establishes an authenticated and encrypted tunnel between itself and the firewall or router at the intranet boundary.

By applying IPSec authentication between the remote client and the firewall or router, you can protect your intranet from unwanted and possibly malicious IP packets. And by encrypting traffic that flows between the remote host and the firewall or router, you can prevent outsiders from eavesdropping on your information.

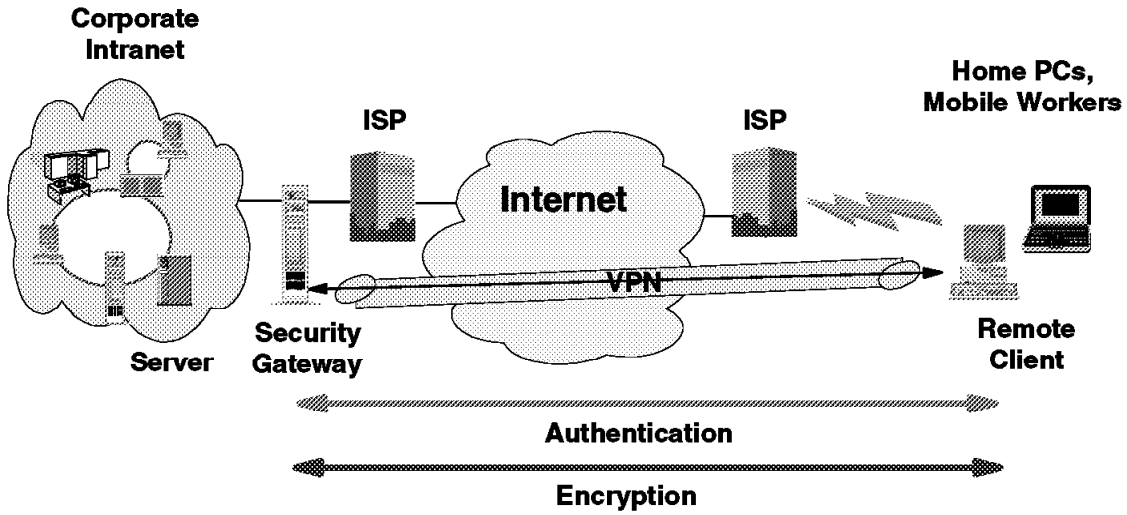


Figure 4. Remote Access Network

The three scenarios discussed in this section are the basis for the IPSec implementation and configuration examples described in this redbook. The next chapter provides step-by-step procedures for configuring IPSec tunnels with IBM Nways Routers. The succeeding chapters provide scenarios on how to implement Data Link Switching (DLSw), IP Bridging Tunnels, Enterprise Extender (HPR over IP), APPN DLUR, TN3270, and Layer 2 Tunneling Protocol (L2TP) through an IPSec tunnel.

Chapter 2. Configuring IPSec with IBM Nways Routers

This chapter explains how to manually configure IPSec tunnels using Nways Multiprotocol Routing Services (MRS) and Nways Multiprotocol Access Services (MAS) V3.1 and V3.2. It also shows the relationship between IP filters and the IPSec feature and explains how IP filters are used by IPSec to direct traffic to and from IPSec tunnels. The chapter concludes with a brief discussion of adding default gateways and static routes to an IPSec configuration.

2.1 Manual IPSec Tunnel Configuration

The following steps are recommended when configuring a manual IPSec tunnel. However, depending on your current router configuration, some of these steps may be omitted. These steps are:

1. Define the router interfaces, the IP addresses and masks.
2. Add packet filters for the router interfaces that will serve as tunnel endpoints.
3. Enable the packet filters.
4. Create an IPSec tunnel endpoint at a router interface.
5. Enable the tunnel.
6. Save the configuration.
7. Restart the router.

Each of these steps is explained in the following sections. As an aid in understanding the different parameters used, we reference the sample network in Figure 5. The examples are based on configuring Router A in the network.

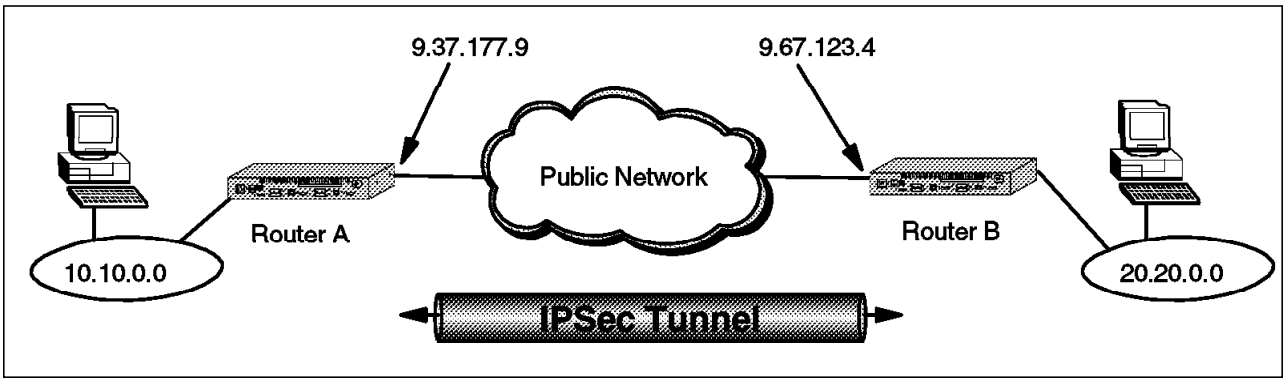


Figure 5. Sample Network Used in IPSec Tunnel Definition

2.1.1 Defining the Router Interfaces

The prerequisite for defining an IPsec tunnel is to configure your hardware interfaces, IP addresses and masks on each router interface that will serve as an IPSec tunnel endpoint. There are multiple ways to accomplish this using both the Config tool and the command line interface from the router console. These methods are not discussed in this redbook. However, Appendix A, “Basic Router Configuration” on page 135 shows one way to do it using the Quick Config command dialog from the router console.

2.1.2 Packet Filters and IPSec

A packet filter is a list of rules (called access controls) used by the router to control the processing of individual packets on an interface. You can define one packet filter for the inbound direction and one for the outbound direction for each interface on the router.

Two new types of access controls were added in MRS/MAS V3.1. Beginning with this version of code, there are now four types of access controls that can be specified in a packet filter. These are:

I - inclusive An access control of type ′I′ means that it is an inclusive filter. In this case, any matched packets will be allowed to proceed through the interface (either in or out depending on the direction of the filter defined.)

E - exclusive An access control of type ′E′ means that it is an exclusive filter. In this case, any matched packets will be dropped from the interface.

S - inclusive This is one of the two new access controls defined in MRS/MAS V3.1. When a match is encountered on an ′S′ filter, the packet is passed to the IPSec engine for processing by the AH and ESP protocols.

N - inclusive This is the other new access control defined in MRS/MAS V3.1. When a match is encountered on an ′N′ filter, the packet is passed to the Network Address Translation (NAT) function for processing.

You can specify multiple access controls on each packet filter. The order of the controls in the access control list is very important because the first access control that is matched is the one that is acted on. In the case of IPSec, this is especially important for transport mode tunnels. (See “Adding Access Controls” on page 12 for more information.)

2.1.2.1 How IPSec Uses Packet Filters

The IPSec architecture defines a Security Policy Database (SPD) that is used to determine which packets should be processed by IPsec. The IPSec implementation in the IBM Nways routers uses the packet filter function as the key element of the SPD. IPSec uses packet filters to *funnel* the packets into and out of the IPSec engine. Both inbound and outbound packet filters are used for this purpose although they work slightly differently in each direction. Figure 6 on page 11 shows conceptually how this process works for IP packets in the outbound direction.

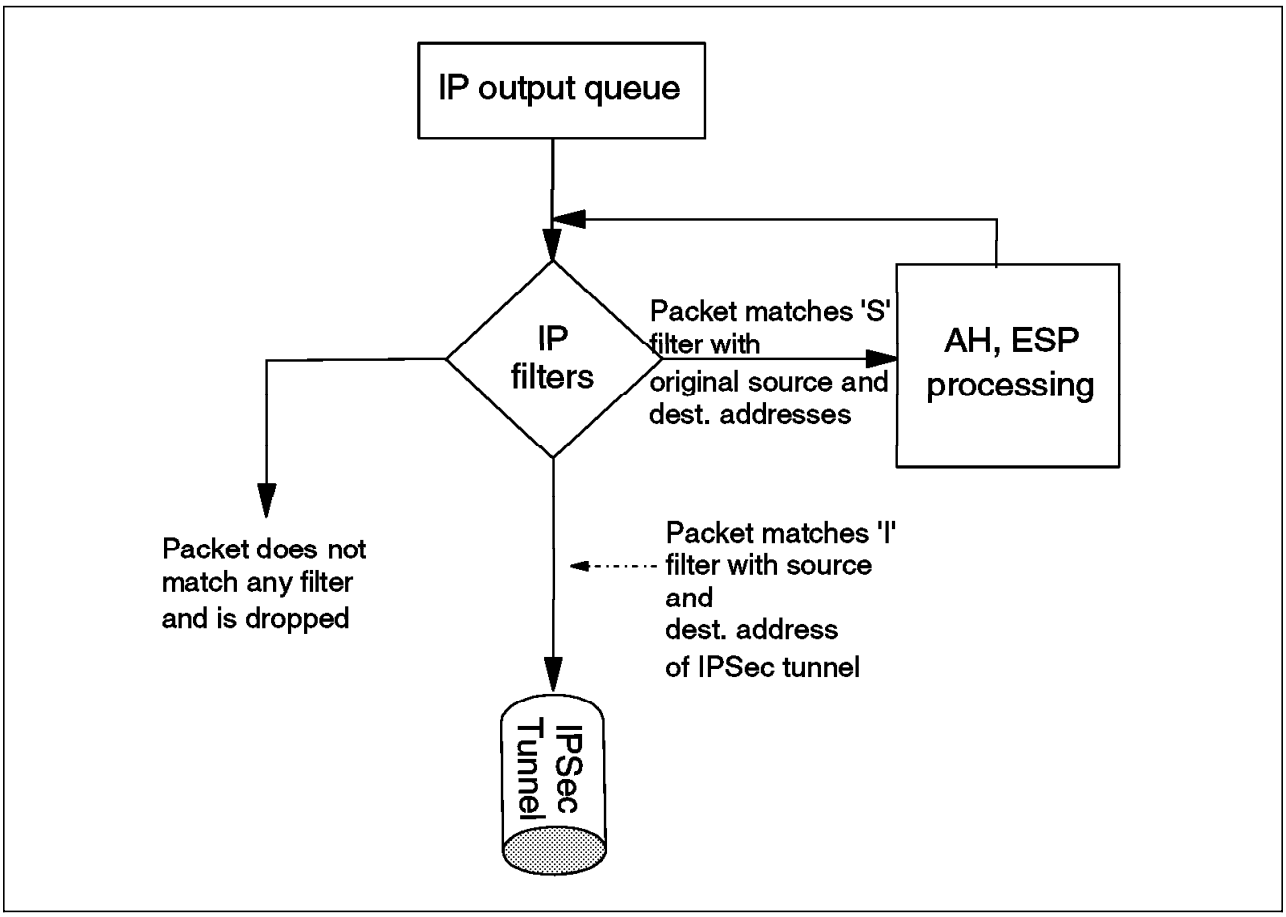


Figure 6. IP Filters and IPSec - Outbound Traffic

As depicted in Figure 6, just before the outbound IP packets leave the router interface, they are tested by the packet filter for that interface. The packet is compared to each access control in the access control list (ACL) for the packet filter one-by-one. If a match is found on an ′S′ type access control, the packet is passed to the IPSec engine for AH/ESP processing.

After IPSec has processed the packet, it puts the packet back through the filters again. This time, the packet must match an inclusive access control (type ′I′) in order for the router to send the packet out on the interface.

Note: As shown in the diagram, if a packet does not match any access control in the list, then the packet is dropped from the interface. This is the primary reason that the second access control is needed in the outbound direction.

2.1.2.2 Defining the Packet Filters

Defining a packet filter is a two-step process. First, you create the packet filter and give it a name. Then, you add access controls to the access control list for that packet filter.

A suggested naming convention for the packet filters is PF_DIR_IFNUM where:

- PF stands for packet filter
- DIR indicates the direction, either in or out
- IFNUM is the interface number in the router

For example, using this convention, a packet filter named PF_IN_0 would indicate an inbound filter on interface 0.

Creating the Filters: You need to define a packet filter for each direction (inbound and outbound) for each interface that will serve as an IPSec tunnel endpoint. Figure 7 shows the Talk 6 command to create a packet filter as well as the command to list the defined packet filters. Note that these commands are issued from within the IP configuration prompt.

Note

The screens in this example show the prompts for configuring packet filters based on a pre-GA version of MRS V3.1. The prompts changed slightly before the the product shipped and they changed again for V3.2. Therefore, depending on the level of code that you are running, your command prompts may look slightly different than the ones shown here. However, the intent of the questions remain consistent with the prompts shown in this example.

```
Config>protocol ip
Internet protocol user configuration
IP config>add pac
Packet-filter name []? pf_out_0
Filter incoming or outgoing traffic? [IN]? out
Which interface is this filter for [0]?
IP config>list pac

List of packet-filter records:

Name               Direction   Interface   State  SRC-Addr-Check
pf_out_0           Out         0           On     N/A

Access Control is: disabled
```

Figure 7. Creating a Filter

Notes:

1. In MRS/MAS version 3.1, a new feature of packet filters was added called Source Address Verification. If enabled, this feature checks to see if the source IP address of the packet matches the subnet for the router interface that the packet is arriving on. If not, the packet is discarded. This helps to block hacking attempts. It is only valid for inbound filters and that is why you see the N/A (not applicable) under the column marked SRC-Addr-Check.
2. Note that when the packet filter is first created, it is *not* enabled. It only becomes active after you enable access control on the router and enable the individual packet filter. (See 2.1.4, “Enabling Packet Filters” on page 18.)
3. You cannot change the name of the filter without losing the details of the access control list. Therefore, be careful when choosing your names for the packet filters.

Adding Access Controls: Once the packet filters have been created, you add access controls to the access control list of the packet filter. Each filter needs two access controls in the list:

- For a tunnel-mode IPSec tunnel, one of the controls specifies the source and destination IP addresses of the tunnel endpoints as well as the IPsec protocols (50 for ESP and 51 for AH). It is a type 'I' (inclusive) control. When this access control is matched on an outbound packet, the packet is allowed to exit the router interface.
- The other access control specifies the network or host IP address(es) that are "funneled" into/out of the tunnel. Its type is 'S' for IPSec. When this access control is matched on an outbound filter, the packet gets sent to the IPSec engine for processing of the AH and ESP protocols.

As stated previously, the order of the controls in the list is important - especially for transport mode tunnels. For example, as can be seen in Figure 6 on page 11, for outbound packets, the first access control that you want the packet to encounter is the type 'S' control. This is necessary so that the packet can be processed by IPSec and the appropriate headers added to the packet before it exits the router.

With transport-mode tunnels, the original IP packet header is used and source and destination IP addresses of the packet, as it traverses the tunnel, are those of the end systems and not the IPSec tunnel endpoints. Therefore, the 'I' access control specifies the same source and destination IP addresses as the 'S' control. In this situation, the only way to distinguish packets that have been through IPSec processing is via the protocol field which will either be 50 or 51, depending on whether you're doing ESP or AH, respectively.

Figure 8 shows the creation of the first of two required access controls. In order to add an access control, the update packet-filter command is issued first and then the add access-control command is used to create the individual access controls for that packet filter. In this case, this access control specifies the tunnel endpoints as source and destination IP addresses for the filter and the IPSec protocols 50 and 51. (See Figure 5 on page 9.) This access control is used to allow IPSec packets to exit the router after they have been processed by IPSec and encapsulated (tunnel-mode tunnels) with the new IP header.

```
IP config>update pac
Packet-filter name []? pf_out_0
Packet-filter 'pf_out_0' Config>add access-control
Enter type [E]? i
Internet source [0.0.0.0]? 9.37.177.9
Source mask [255.255.255.255]?
Internet destination [0.0.0.0]? 9.67.123.4
Destination mask [255.255.255.255]?
Enter starting protocol number ([0] for all protocols) [0]? 50
Enter ending protocol number [50]? 51
Enable Logging?(Yes or [No]):
Packet-filter 'pf_out_0' Config>
```

Figure 8. Adding an Access Control to a Packet Filter

Figure 9 on page 14 shows the addition of the second IPSec required access control to the outbound filter. This control specifies the network or host IP address(es) that will be *funneled* into the IPSec tunnel. Referring to Figure 5 on page 9, these subnetwork addresses are the token-ring segments that are

attached to each router and represent the private intranet segments that we are trying to connect via our VPN. When this access control is matched, the outbound packets are directed to the IPSec engine for AH and ESP processing. Note that for this access control, the protocol field and the port numbers are not specified because we want *all* protocols to be processed by IPSec and sent through the tunnel.

The tunnel ID specified needs to match the ID that will be specified during the creation of the IPSec tunnel. (See 2.1.5, “Defining the IPSec Tunnel” on page 19.)

```
Packet-filter 'pf_out_0' Config>add access-control
Enter type [I]? S
Internet source [0.0.0.0]? 10.10.0.0
Source mask [255.255.255.255]? 255.255.0.0
Internet destination [0.0.0.0]? 20.20.0.0
Destination mask [255.255.255.255]? 255.255.0.0
Enter starting protocol number ([0] for all protocols) [0]?
Enter IPsec Tunnel ID [1]? 100
Enable Logging(Yes or [No]):
Packet-filter 'pf_out_0' Config>
```

Figure 9. Adding the Second Access Control to the Packet Filter

This completes the definition of the outbound packet filter and the two IPSec required access controls.

2.1.3 Defining the Inbound Packet Filter

In addition to the outbound filter, you must also define a packet filter for the inbound direction. Like the outbound filter, the inbound filter needs two access controls. However, the purpose of the access filters is slightly different for the inbound direction. Figure 10 on page 15 shows conceptually how this process works for IP packets in the inbound direction.

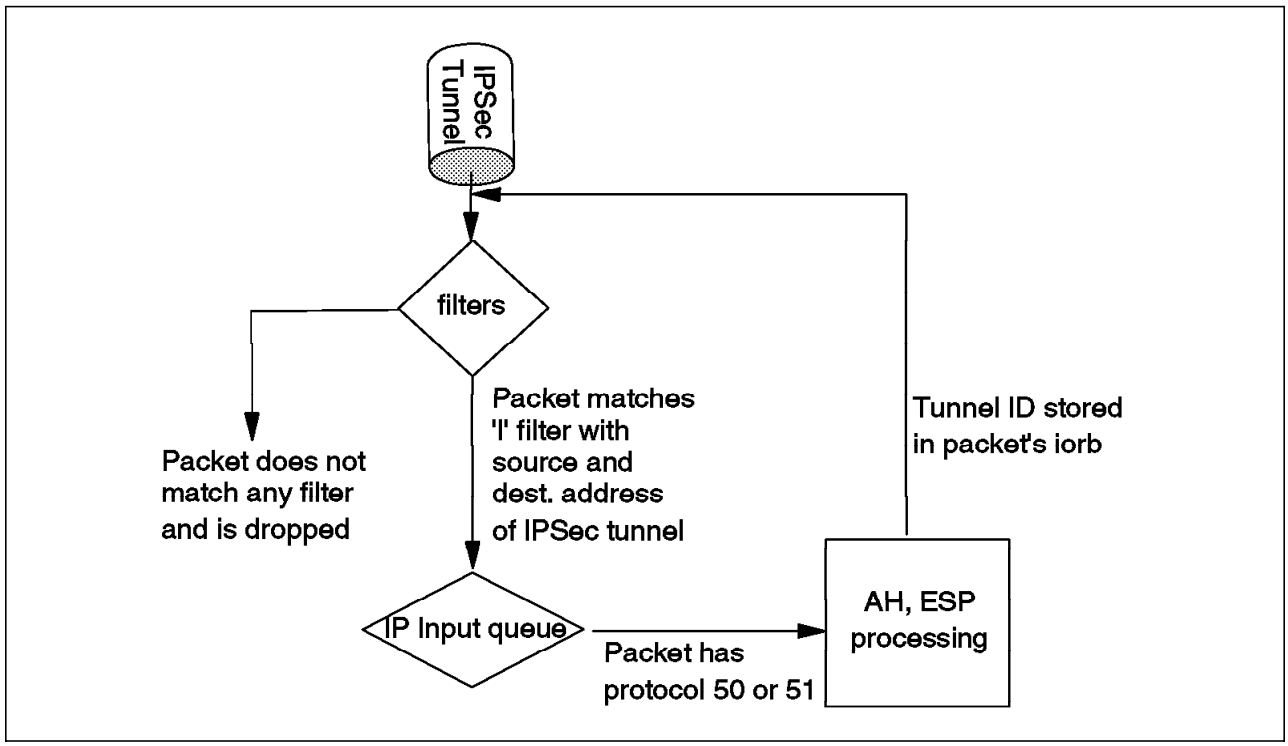


Figure 10. IP Filters and IPSec - Inbound Traffic

As packets come into the interface, the process that was used in the outbound direction at the ingress of the IPSec tunnel needs to be reversed. As can be seen in the figure, we want the packet to first match an access control of type ′I′ with source and destination addresses of the IPSec tunnel endpoints. (Remember that when using IPSec in tunnel mode, the packets get encapsulated with a new IP header. The source and destination addresses that get put into this new header are the tunnel starting and ending points.)

This control also specifies IPSec protocols 50 and 51, but for the purpose of checking to make sure they are really IPSec packets - not so that they can be routed to the IPSec engine. The packets get routed to IPSec by the protocol demux logic when that function sees that they have a protocol field of 50 or 51. This works exactly the same way as a TCP or UDP packet gets routed to the TCP or UDP code.

When the packet is passed to IPSec, the AH and ESP headers are processed, the packet is authenticated and/or decrypted and the tunnel ID is stored in the packet′s iorb. The packet is then sent back through the filters - the same as it works for the outbound direction. Figure 11 on page 16 shows conceptually how the packet is processed the second time through the filters.

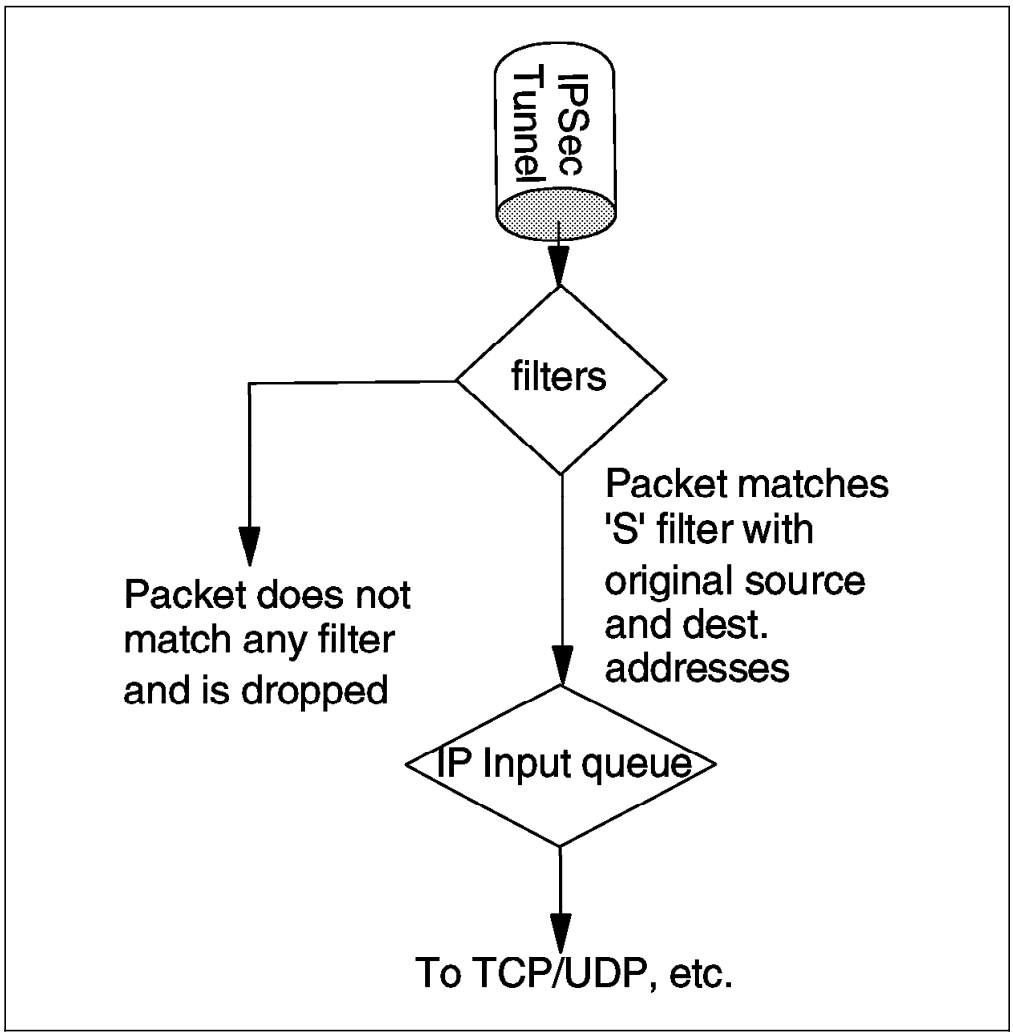


Figure 11. The Second Time through the Inbound Packet Filter

This time, the packet needs to match a control of type ′S′. When this occurs, the filter checks the tunnel ID that was received with the IPSec packet against the ID that was configured in the access control. These two tunnel IDs have to match or the packet is dropped. If they match, the packet is allowed to proceed to either the local IP queue (if the decapsulated packet is for local services such as TCP) or is routed to another interface (if the packet is not for local services).

2.1.3.1 Changing Access Controls in a Packet Filter

There are several other useful commands that can be used to modify a packet filter once it has been created. One gives you the ability to modify the data on the access control. Another command gives you the ability to change the order of the controls in the access control list. Finally, there is a command to delete an access control from the list. These commands are described in the following sections.

Modifying the Data: To modify the data in an access control, first issue the update command for the packet filter, then issue the change command. This is illustrated in Figure 12 on page 17, Figure 13 on page 17, and Figure 14 on page 18. First the update command is issued followed by the list command to see the current access controls that are in the list.

```
IP config>update pac
Packet-filter name []? pf_out_0
Packet-filter 'pf_out_0' Config>list acc
Access Control is: disabled
Access Control facility: USER

List of access control records:

1   Type=I     Source=9.37.177.9       Dest=9.67.123.4       Prot= 50-51
               Mask=  255.255.255.255  Mask=255.255.255.255
               SPorts=    0-65535      DPorts=    0-65535      Log=No

2   Type=I     Source=10.10.0.0        Dest=10.20.0.0        Prot=  0-255
               Mask=  255.255.255.255  Mask=255.255.255.255
               SPorts=    0-65535      DPorts=    0-65535
               ACKO=N  T/C= **/**      Log=No
```

Figure 12. Listing Access Controls on a Packet Filter

Then the change command is issued to change one of the controls. Here, we change the type from an ordinary inclusive control to an IPSec control. Note that one of the parameters for an 'S' control is the IPSec tunnel ID. This parameter is not necessary for an ordinary inclusive control.

```
Packet-filter 'pf_out_0' Config>change acc
Enter index of access control to be changed [1]? 2
Enter type [I]? S
Internet source [10.10.0.0]?
Source mask [255.255.255.255]?
Internet destination [10.20.0.0]?
Destination mask [255.255.255.255]?
Enter starting protocol number ([0] for all protocols) [0]?
Enter Secured Tunnel ID [0]? 100
Enable Logging?(Yes or [No]):
Packet-filter 'pf_out_0' Config>
```

Figure 13. Changing an Access Control

Finally, the access control list (ACL) is redisplayed to make sure the change took effect. You can see that the type for control number two was changed from 'I' to 'S'.

```
Packet-filter 'pf_out_0' Config>list acc
Access Control is: disabled
Access Control facility: USER

List of access control records:

1   Type=I     Source=9.37.177.9       Dest=9.67.123.4       Prot= 50-51
               Mask=  255.255.255.255  Mask=255.255.255.255
               SPorts=    0-65535      DPorts=    0-65535
                                       Log=No

2   Type=SI    Source=10.10.0.0        Dest=10.20.0.0       Prot=  0-255
               Mask=  255.255.255.255  Mask=255.255.255.255
               SPorts=N/A              DPorts=N/A            Tid=100
                                       Log=No

Packet-filter 'pf_out_0' Config>
```

Figure 14. Verifying the Change

Changing the Order of Access Controls: You can use the move access-control command to change positions of the controls in the ACL. Figure 15 gives an example of using this command.

```
2210 Packet-filter 'pf_out_0' Config>move access-control 4 1
About to move:

4   Type=I S   Source=192.168.157.0    Dest=9.24.105.0       Prot=  0-255
               Mask=  255.255.255.0    Mask=255.255.255.0
               SPorts=N/A              DPorts=N/A            Tid=1
                                       Log=No
to be after:

1   Type=I S   Source=192.168.157.0    Dest=192.168.180.0    Prot=  0-255
               Mask=  255.255.255.0    Mask=255.255.255.0
               SPorts=N/A              DPorts=N/A            Tid=1
                                       Log=No
Are you sure this is what you want to do(Yes or [No]): yes
2210 Packet-filter 'pf_out_0' Config>exit
```

Figure 15. Changing the Order of the Access Controls in the ACL

Deleting an Access Control: To delete an access control, use the delete access-control command from within the update-packet-filter command.

2.1.4 Enabling Packet Filters

In order for the packet filter to be active, the access control function has to be enabled at the box level and each packet filter must be enabled by name. Figure 16 on page 19 shows an example of both of these commands which are self explanatory. Note that these commands are both issued from the Talk 6 IP config prompt.

```
IP config>set access-control on
IP config>enable packet-filter
Enter packet-filter name to be enabled []? pf_out_0
IP config>enable packet-filter
Enter packet-filter name to be enabled []? pf_in_0
```

Figure 16. Enabling Access Control and Individual Packet Filters

It is a good idea to check to make sure that the filters are enabled. One way to verify that the filter is enabled is to use the update command for a packet filter and then list the access controls. This will tell you whether the access control is enabled for that packet filter. An example of this is shown in Figure 17.

```
IP config>update pac
Packet-filter name []? pf_out_0
Packet-filter 'pf_out_0' Config>list acc
Access Control is: enabled
Access Control facility: USER

List of access control records:

1   Type=I     Source=9.37.177.9       Dest=9.67.123.4       Prot= 50-51
               Mask=  255.255.255.255  Mask=255.255.255.255
               SPorts=    0-65535      DPorts=    0-65535
                                       Log=No

2   Type=I S   Source=10.10.0.0        Dest=10.20.0.0        Prot=  0-255
               Mask=  255.255.255.255  Mask=255.255.255.255
               SPorts=N/A              DPorts=N/A            Tid=100
                                       Log=No

Packet-filter 'pf_out_0' Config>
```

Figure 17. Checking That the Packet Filter Is Enabled

After making changes to the access controls, you need to reset IP to make the changes effective and also to clear the access control cache. However, in this example, we wait until the IPSec tunnel has been defined and then we perform a restart of the router. This activates both the changes to the filters and IPSec at the same time.

2.1.5 Defining the IPSec Tunnel

This section describes the procedure to create the IPSec tunnel between two routers for a VPN over the public network.

Important Note

This section assumes a working knowledge of the IPSec architecture. A basic explanation is given for each of the required parameters. However, if you are not familiar with the IPSec architecture, it is strongly recommended that you reference the companion redbook in this series entitled *A Comprehensive Guide to Virtual Private Networks, Volume I: IBM Firewall, Server and Client Solutions,* SG24-5201 for more information.

IPSec tunnel configuration is performed from the IPSec feature menus under talk 6. For each IPSec tunnel, you give it a name, define the tunnel characteristics, and then enable the tunnel. While the dialog to add a tunnel is initiated with just one command, we have broken up the dialog into several pieces to provide some explanation at key points in the dialog.

The first part of the dialog defines the tunnel name, ID, tunnel lifetime, encapsulation mode, and tunnel policy.

```
RTR-A IPsec config>add tun
Tunnel ID (1-65535) [1]? 100
Tunnel Name (optional) []? ah_test
Tunnel Lifetime, in minutes (0-525600) [46080]?
Tunnel Encapsulation Mode (TUNN or TRANS) [TUNN]?
Tunnel Policy (AH,ESP,AH_ESP,ESP_AH) [AH_ESP]? AH
```

Figure 18. Defining the Tunnel

Notes:

1. When you define the tunnel, you are defining two IPSec Security Associations (SAs), one in each direction. (Remember that an IPSec tunnel consists of two uni-directional security associations between the tunnel endpoints.)
2. The tunnel ID here must be the same as specified when the access control was created. (See Figure 9 on page 14.)
3. Once created, the tunnel name cannot be changed.
4. The tunnel lifetime defaults to 46080 minutes which converts to 32 days. The maximum is 525600 minutes which is one year.
5. The tunnel encapsulation mode can be set to either tunnel mode or transport mode per the IPSec architecture. Tunnel mode is the normal case between routers that are using the public network to create a VPN. Transport mode is used to create a tunnel between two end stations.

   The difference between the two modes is that with tunnel mode, the entire original IP packet is encapsulated within a new IP packet. This new packet has IP source and destination addresses of the tunnel endpoints. With transport mode, the original IP header is used with the original source and destination IP addresses.
6. From Figure 18, you can see that there are four choices for the tunnel policy:

   AH This is the choice if you want to perform only authentication (the IPSec AH protocol) on packets going over this tunnel.

ESP This is the choice if you want to perform encryption (the IPSec ESP protocol) on packets going over this tunnel. Note that if you make this selection, you can also do authentication on the packets since the ESP protocol has an optional authentication feature.

AH_ESP This is the choice if you want to perform encryption and authorization using both the IPSec ESP and AH protocols. This selection indicates that for packets in the outbound direction, the packets will be encrypted first via the ESP protocol, then the AH algorithms will be run on the encrypted payload.

ESP_AH tunnel, defined This choice also allows you to do both encryption and authorization using both the IPSec ESP and AH protocols. However, the order is reversed. With this selection, packets in the outbound direction will go through the AH algorithms first, then they will be encrypted via the ESP protocol.

Take Note

If you are ever trying to configure a tunnel policy and the only choice is AH, then you either don't have a code load with encryption or you are working on a 2216 where the `load add package encryption` command has not yet been specified. (Encryption is supplied as a separate load module for MAS and the `load add package encryption` command specifies that this module should be loaded as part of the normal IPL process.) This command only needs to be issued once.

At this point, the basic tunnel has been defined. Since we specified that this tunnel will use AH, the dialog now prompts us for the parameters that the AH algorithms will use. Figure 19 shows an example of these prompts.

```
Local IP Address [192.168.182.1]? 9.37.177.9
Local Authentication SPI (1-65535) [666]? 333
Local Authentication Algorithm (HMAC-MD5,HMAC-SHA) [HMAC-MD5]?
Local Authentication Key (32 characters) in Hex (0-9,a-f,A-F):
Enter Local Authentication Key again (32 characters) in Hex (0-9,a-f,A-F):
```

Figure 19. Defining AH Parameters - Local End of the Tunnel

Notes:

1. This first series of prompts are for the AH parameters at the local end of the tunnel (the router you're configuring which is Router A in Figure 5 on page 9 in this example). The parameters in local authentication must be the same as the parameters in remote authentication of the router at the other side of tunnel. For example, if you choose the HMAC-MD5 algorithm for the local authentication algorithm, then you must configure HMAC-MD5 as the other router's *remote* AH algorithm. In effect, you are defining parameters for two uni-directional Security Associations (SAs) and each tunnel endpoint must agree on the parameters used for each SA. (Remember that two SAs exist for each IPSec tunnel: one in each direction.)

2. You can use different parameters for the SAs in each direction. However, the parameters specified for each SA have to match at each end of the IPSec tunnel. For example:
   - The local key entered in router A must match the remote key entered in router B.
   - The remote key entered in router A must match the local key entered in router B.

   The same principle holds true for the SPI and the AH algorithm specified.

   With this said, however, we recommend that you use the same parameters for both SAs unless you have a good reason to do otherwise.
3. SPI is the security parameter index. You can think of this as an index into the database where the parameters for this tunnel will be stored.
4. In this version of MRS/MAS, we are using manual key configuration. This means that we manually enter the keys that will be used for the AH and ESP algorithms. We use simple keys in this example. In future versions of MRS/MAS, we will have the capability to use ISAKMP/Oakley, the automated key management protocols that will set the keys and refresh them periodically. The IPSec architecture specifies ISAKMP/Oakley as the protocols to use for its Integrated Key Exchange (IKE) framework.
5. In total, you have to enter four keys when configuring AH:
   - Local key in router A
   - Remote key in router A
   - Local key in router B
   - Remote key in router B
6. Also remember that each of the above keys must be typed twice to prevent mistakes. At the time of this writing, any typing mistakes will terminate the add tunnel command and you must start over.

After these parameters have been entered, the prompts switch to questions about the AH parameters for the remote end of the tunnel. As you might expect, the parameters entered for remote authentication must match parameters entered for local authentication of the router at the other side of the tunnel. For example, if you specify at the far end that outgoing packets should use the HMAC-MD5 algorithm to generate the Integrity Check Value (ICV), then you need to specify that incoming packets here at this end of the tunnel will be authenticated using the same HMAC-MD5 algorithm (and the same key). This is the idea behind configuring the parameters used at the remote end here at the local end of the tunnel. Figure 20 shows an example of these prompts.

```
Remote IP Address [0.0.0.0]? 9.67.123.4
Remote Authentication SPI (256-65535) [256]? 666
Remote Authentication Algorithm (HMAC-MD5,HMAC-SHA) [HMAC-MD5]
Remote Authentication Key (32 characters) in Hex (0-9,a-f,A-F):
Enter Remote Authentication Key again (32 characters) in Hex (0-9,a-f,A-F):
Enable replay prevention? [No]:
Do you wish to enable this tunnel? [Yes]:
```

Figure 20. Defining AH Parameters - Remote End of the Tunnel

The IPSec architecture defines a technique for ensuring that a hacker cannot intercept a datagram and play it back at some later time without being detected. This is called anti-replay or replay prevention support. As per the architecture, MRS/MAS implements this support via the use of a sequence number that is included in the AH header of every packet. If enabled, the receiving side of the SA checks all sequence numbers on incoming packets to make sure that they fall within a window and have not been received previously. The sequence number is a 32-bit field in the header and is initialized to zero at the inception of the SA.

For manual IPSec implementations such as MRS/MAS V3.1 and V3.2, it is not recommended to enable anti-replay support. This is due to the fact that the architecture stipulates that the sequence number cannot wrap when it reaches the highest number in the range (2^{32}=4.29 billion packets). This means that if you enable anti-replay support, you have to ensure that the SA is re-established every 4.29 billion packets. When MRS/MAS implement ISAKMP/Oakley, there will be automated ways to refresh the SAs and hence this will not be a restriction.

After the tunnel definition is completed, you can list the definition back out to check for errors such as mis-typed IP addresses. Figure 21 shows an example of this command.

```
IPsec config>list tunnel all

   ID         Name          Local IP Addr   Remote IP Addr   Mode    State
 ------  ---------------  ---------------  ---------------  -----  --------
    100  ah_test          9.37.177.9       9.67.123.4       TUNN   Enabled
```

Figure 21. Listing a Tunnel Definition

2.1.6 Enabling IPSec on the Router

IPSec must be enabled in order for the tunnel to become active. Figure 22 shows an example of this command which is performed from the Talk 6 IPSec feature prompt. As the figure shows, you can check the status of IPSec and the status of each tunnel with the list all command.

```
IPsec config>enable ipsec
IPsec config>list all

IPsec is ENABLED

   ID         Name          Local IP Addr   Remote IP Addr   Mode    State
 ------  ---------------  ---------------  ---------------  -----  --------
    100  ah_test          9.37.177.9       9.67.123.4       TUNN   Enabled
```

Figure 22. Listing the IPSec Status

Whenever you make a change to an IPSec tunnel (or add a new definition), you need to reset the IPSec feature to make the changes effective. However, in this example, we restart the router in the next step which both resets IPSec and also activates the changes to the access controls that we made in 2.1.3, “Defining the Inbound Packet Filter” on page 14.

2.1.7 Saving the Configuration

Now that the tunnel has been created, you need to save the changes to the configuration and reload (2216) or restart (2210) the router. This will activate both the changes to the access controls and to the IPSec feature.

The procedure to do this is slightly different for the 2210 and the 2216.

If you are using a 2210, the configuration is automatically written to the CONFIG area in Flash memory as you make the configuration changes. Therefore, you do not have to explicitly perform a save operation.

If you are using a 2216, you need to write the configuration to the hard disk to save it. An example of this operation is shown in Figure 23.

```
Config>write
Config Save: Using bank A and config number 2
```

Figure 23. Saving the Configuration on a 2216

2.1.8 Restarting the Router

Next, restart the router to make the configuration changes active. On a 2216, use the reload command as shown in Figure 24.

```
Config>reload
Are you sure you want to reload the gateway? (Yes or [No]): y
```

Figure 24. Restarting the 2216

On the 2210, use the restart command as shown in Figure 25 on page 25. Note that this command is performed from the main router prompt. (Press <CNTRL><P> to get to this prompt.)

```
*restart
Are you sure you want to restart the gateway? (Yes or [No]): y

Copyright Notices:

Licensed Materials - Property of IBM
Multiprotocol Routing Services
(C) Copyright IBM Corp. 1996
All Rights Reserved. US Gov. Users Restricted Rights -
Use, duplication or disclosure restricted
by GSA ADP Schedule Contract with IBM Corp.

MOS Operator Control

*
```

Figure 25. Restarting the Router (2210)

2.1.9 Defining an IPSec Tunnel Using Encryption (ESP)

The procedure for configuring a tunnel that uses ESP is very similar to that for creating a tunnel with the AH protocol. However, instead of defining parameters that relate to the AH protocol, you define parameters for the ESP protocol, for example, the encryption algorithm.

Important Note

Encryption is an optional feature in MRS/MAS. If your software load does not include encryption, you will not see encryption related parameters when configuring the IPSec feature.

Also, on the 2216, the encryption load module must be specified to be loaded during the IPL of the router. You specify this via the ″load add package encryption″ command.

We illustrate the configuration of an ESP tunnel below by changing the tunnel configuration that we created in 2.1.5, “Defining the IPSec Tunnel” on page 19 to specify ESP instead of AH. We use the ″change tunnel″ command to make these changes to the existing tunnel configuration. As in the AH example, we break up the dialog into several figures to provide some explanation of the parameters. Figure 26 shows an example of these prompts.

```
RTR-A IPsec config>chan tun
Tunnel ID or Tunnel Name []? 100
Tunnel Lifetime, in minutes (0-525600) [46080]?
Tunnel Encapsulation Mode (TUNN or TRANS) [TUNN]?
Tunnel Policy (AH,ESP,AH-ESP,ESP-AH) [AH]? esp
```

Figure 26. Changing an IPSec Tunnel Definition

Like AH, ESP configuration requires parameters for the local and remote ends of the tunnel. First, you are prompted for the parameters for the local end. Also like AH, the parameters for the local end must be the same as the parameters in the other router's remote parameters.

Like AH, there are four keys to configure. However, as mentioned previously, the IPSec ESP protocol does allow you to do authentication as part of ESP processing. If you specify to do authentication as part of ESP, then you will have to configure additional keys for the authentication. (See the last question in the dialog below.) Figure 27 shows an example of these prompts.

```
Local IP Address [9.37.177.9]?
Local Encryption SPI (256-65535) [256]? 444
Local Encryption Algorithm (DES-CBC,CDMF,3DES) [DES-CBC]?
Local Encryption Key (16 characters) in Hex (0-9,a-f,A-F):
Enter Local Encryption Key again (16 characters) in Hex (0-9,a-f,A-F):
Additional Padding for local Encryption (0-120) [0]?
Do you wish to use local ESP authentication? [No]:
```

Figure 27. Defining the Local ESP Parameters

Depending on the country you are in, you may not have all the options shown above for the encryption algorithms. IBM is restricted by the U.S. Government in exporting Triple DES (3DES) and not all countries allow DES-CBC to be imported. For these reasons, there are different MRS/MAS loads with different encryption algorithms embedded that are used for export.

The additional padding feature can be used to extend the size of the ESP payload in order to help prevent a hacker from knowing the true size of the data being encrypted. You can specify up to 120 bytes of additional padding for each packet.

As mentioned previously, you can also specify to perform authentication as part of ESP processing. When you do authentication in ESP instead of AH, the coverage on the part of the packet that is authenticated is not quite as good as it is on packets that are authenticated with the AH protocol. When using ESP authentication, only the part of the packet from the ESP header to the ESP trailer gets authenticated. With AH authentication, the entire IP packet is authenticated. (Please see *A Comprehensive Guide to Virtual Private Networks, Volume I: IBM Firewall, Server and Client Solutions,* SG24-5201 for more information.)

Next, you will define the parameters for the remote end of the tunnel. Again, the parameters entered here for the remote side must be the same as the parameters entered at the other router for its local encryption. Figure 28 on page 27 shows an example of these prompts.

```
Remote IP Address [9.67.123.4]?
Remote Encryption SPI (1-65535) [777]? 777
Remote Encryption Algorithm (DES-CBC,CDMF,3DES) [DES-CBC]?
Remote Encryption Key (16 characters) in Hex (0-9,a-f,A-F):
Enter Remote Encryption Key again (16 characters) in Hex (0-9,a-f,A-F):
Do you wish to perform verification of remote encryption padding? [No]:
Do you wish to use remote ESP authentication? [No]:
Do you wish to enable this tunnel? [Yes]:
RTR-A IPsec config>
```

Figure 28. Defining the Remote ESP Parameters

Now we need to reset the IPSec feature to activate the changes in the existing tunnel. This is performed from the Talk 5 IPSec menus. You do not have to reload or restart the router. Figure 29 shows how to do this.

```
RTR-A IPsec>reset ipsec
IPsec has been reset
```

Figure 29. Resetting the IPSec Feature to Activate Changes

2.1.10 Monitoring Status

You can monitor the status of the IPSec from the talk 5 menus. The ″list tunnel active″ command shows the information of active IPSec tunnels. You can specify to see a specific tunnel or you can see the information for all active tunnels. An example is shown in Figure 30 on page 28 for tunnel number 1. Note that this example shows the AH tunnel configured in 2.1.5, “Defining the IPSec Tunnel” on page 19.

```
RTR-A >f ipsec
RTR-A IPsec>list tunnel active 1
Tunnel       Name        Mode   Policy   Life   Replay        Tunnel
  ID                                             Prev       Expiration
------  ---------------  -----  ------  ------  ------  ------------------
   100  ah_test          TUNN   AH       46080    No    15:40  Jul  6 1998

Local Information:
      IP Address: 9.37.177.9
  Authentication:  SPI:   333    Algorithm: HMAC-MD5
      Encryption:  SPI: -----    Encryption Algorithm: --------
                                 Extra Pad: ---
                                 ESP Authentication Algorithm: ----------
Remote Information:
      IP Address: 9.67.123.4
  Authentication:  SPI:   666    Algorithm: HMAC-MD5
      Encryption:  SPI: -----    Encryption Algorithm: --------
                                 Verify Pad?: ---
                                 ESP Authentication Algorithm: ----------
```

Figure 30. Listing Tunnel Information from Talk 5

The stat command shows you the number of packets sent and received through IPSec. You can specify a tunnel name or number to see statistics for just one tunnel or you can get the global statistics for all the IPSec tunnels currently active in the router. Figure 31 shows an example of listing the global statistics. In this case, there is only one tunnel defined - the same AH tunnel that was defined above.

```
RTR-A IPsec>stat
Enter the Tunnel ID, Tunnel Name, or 'ALL' [ALL]?

                          Global IPSec Statistics
Received:
  total pkts   AH packets   ESP packets   total bytes    AH bytes     ESP bytes
  ----------   ----------   -----------   -----------   ----------   ----------
          96           96             0          9984         9984            0

Sent:
  total pkts   AH packets   ESP packets   total bytes    AH bytes     ESP bytes
  ----------   ----------   -----------   -----------   ----------   ----------
         102          102             0         10608        10608            0

Receive Packet Errors:
  total errs    AH errors   AH bad seq   ESP errors   ESP bad seq
  ----------   ----------   ----------   ----------   -----------
           0            0            0            0             0

Send Packet Errors:
  total errs    AH errors   ESP errors
  ----------   ----------   ----------
           0            0            0
```

Figure 31. Listing Tunnel Statistics

Figure 32 on page 29 shows an example of the list tunnel active command for an ESP tunnel.

```
RTR-A IPsec>list tun act
Enter the Tunnel ID, Tunnel Name, or 'ALL' [ALL]? 100

Tunnel       Name        Mode   Policy   Life   Replay        Tunnel
  ID                                            Prev       Expiration
------  ---------------  -----  ------  ------  ------  ------------------
   100  ah_test          TUNN   ESP      46080    No    10:06  Jul 18 1998

Local Information:

      IP Address: 9.37.177.9
  Authentication:  SPI: -----    Algorithm: ----------
      Encryption:  SPI:   444    Encryption Algorithm: DES-CBC
                                 Extra Pad:   0
                                 ESP Authentication Algorithm: ----------
Remote Information:

      IP Address: 9.67.123.4
  Authentication:  SPI: -----    Algorithm: ----------
      Encryption:  SPI:   777    Encryption Algorithm: DES-CBC
                                 Verify Pad?:  No
                                 ESP Authentication Algorithm: ----------
```

Figure 32. Listing Tunnel Information from Talk 5

Figure 33 shows an example of the stat command for the same ESP tunnel in the previous figure. Note that in this case, tunnel 1 is an ESP tunnel and so there are statistics for ESP packets while there are no occurrences of AH packets reported.

```
RTR-A IPsec>stat
Enter the Tunnel ID, Tunnel Name, or 'ALL' [ALL]? 100

Statistics For Secure Tunnel 1
Received:
  total pkts   AH packets   ESP packets   total bytes    AH bytes     ESP bytes
  ----------   ----------   -----------   -----------   ----------   ----------
          25            0            25          2500            0         2500
Sent:
  total pkts   AH packets   ESP packets   total bytes    AH bytes     ESP bytes
  ----------   ----------   -----------   -----------   ----------   ----------
          25            0            25          1600            0         1600
Receive Packet Errors:
   AH errors   AH bad seq   ESP errors   ESP bad seq
  ----------   ----------   ----------   -----------
           0            0            0             0
Send Packet Errors:
   AH errors   ESP errors
  ----------   ----------
           0            0
```

Figure 33. Listing Tunnel Information from Talk 5

Another important method of monitoring an IPSec tunnel is to check the packet filters at the tunnel endpoints to see how many times they have been invoked. The packet-filter command is used for this and is issued from the talk 5 IP prompt as shown in Figure 34 on page 30 for an example packet filter named pf_in_0.

Note: Figure 34 is just an example screen and does not relate to the example IPSec tunnel defined in this chapter.

```
RTR-A IP>packet-filter pf_in_0
Name              Dir  Intf  State  Src-Addr-Ver  #Access-Controls
pf_in_0           In   0     On     Off           3

Access Control currently enabled
Access Control facility: USER

Access Control run 1687 times, 9335 cache hits

List of access control records:

1   Type=I     Source=192.168.189.59   Dest=192.168.189.1    Prot= 50-51
               Mask=  255.255.255.255  Mask=255.255.255.255  Use=4
               SPorts=    0-65535      DPorts=    0-65535
                                       Log=No

2   Type=I S   Source=192.168.189.59   Dest=192.168.189.1    Prot=  0-255
               Mask=  255.255.255.255  Mask=255.255.255.255  Use=2
               SPorts=N/A              DPorts=N/A            Tid=1
                                       Log=No

3   Type=I S   Source=192.168.157.0    Dest=192.168.180.0    Prot=  0-255
               Mask=  255.255.255.0    Mask=255.255.255.0    Use=2
               SPorts=N/A              DPorts=N/A            Tid=1
                                       Log=No
```

Figure 34. Displaying the Number of Invocations of an Access Control

The Use=x shows how many times each access control has been matched. If your filters are defined correctly, you should see these numbers increasing as traffic is being sent through the tunnel.

These counters are reset every time the router is IPLed or the IP protocol is reset.

2.2 IP Routing Considerations

When using a public network such as the Internet to create a VPN as illustrated in Figure 5 on page 9, you will not be able to run a dynamic routing protocol between the routers at the endpoints of the IPSec tunnel.

Without setting any explicit routing, the routing code will route to any subnet that it is aware of based on the IP address and subnet mask specified at the physical interfaces. This means that the router knows how to route to IP addresses located within the subnets associated with its interfaces with no explicit configuration.

If the ultimate IP destination is not on one of the subnets on the router's interfaces then the router must obtain a route to the next-hop router. Since we cannot run RIP or OSPF over a public network, we have to either set a default gateway (all IP traffic that does not belong in an attached subnet is sent to the default gateway) or set static (explicit) routes.

If the router is the start of a tunnel, the next-hop router is either the IP address of the start of the tunnel, that is, an IP address on that router, or the IP address of the next router. Both approaches appear to work. However, it is recommended that the IP address of the next router be used.

2.2.1 Setting a Default Gateway

The router will send all traffic that is not destined to a subnet that is attached directly to the router to the default gateway. Figure 35 shows an example of defining a default gateway.

```
Config>protocol ip
Internet protocol user configuration
IP config>set default network-gateway
Default gateway []? 2.2.2.2
gateway's cost [1]?
IP config>
```

Figure 35. Setting the Default Gateway

2.2.2 Setting Static Routes

The static route is the address of the next router (next hop) that a packet with a given IP address or a packet belonging to a particular subnet should be routed to. In the following example, all packets destined for network 4.4.4.X will be sent to the router whose address is 2.2.2.2. The router, knowing its own interface addresses and the subnets associated with each interface address, will determine which physical port to route the packet to. Figure 36 shows an example of defining a default gateway.

```
IP config>add route
IP destination []? 4.4.4.0
Address mask [255.0.0.0]? 255.255.255.0
Via gateway 1 at []? 2.2.2.2
Cost [1]?
Via gateway 2 at []?
IP config>
```

Figure 36. Adding a Static Route

Now, to list the static routes that have been defined, use the list command as shown in Figure 37 on page 32.

```
IP config>list routes
route to  4.4.4.0      ,255.255.255.0     via  2.2.2.2       cost 1
IP config>
```

Figure 37. Listing the Static Routes

Chapter 3. Connecting the Data Center to the Branch Office

As discussed in 1.2, “VPN Customer Scenarios” on page 3, one application of VPNs is in connecting branch office intranets to a central site (perhaps a mainframe data center) via a non-secured public network such as the Internet. In this section of the redbook, we provide step-by-step procedures for implementing such a scenario using the IPSec feature of the IBM Nways 2210/2216 routers.

In this chapter, we configure a secure tunnel to establish basic TCP/IP connectivity between the branch office intranet and the central intranet located in the corporate data center.

Then, in subsequent chapters, we extend the configuration of the routers so that more protocols and features make use of the secure connection between the intranet sites. The following protocols and features are demonstrated:

1. DLSw for NetBIOS and SNA
2. Bridging tunnel for LAN-to-LAN bridging over TCP/IP
3. HPR over IP
4. APPN DLUR function
5. TN3270E server function

3.1 Description of the Environment

Figure 38 shows our configuration used to implement the scenario. As can be seen in the figure, the main intranet site consists of two Ethernet LAN segments, one token-ring, as well as a channel attached S/390. The main site is connected to the Internet with an IBM 2216. The branch office intranet consists of a token-ring LAN and is connected to the Internet with an IBM 2210.

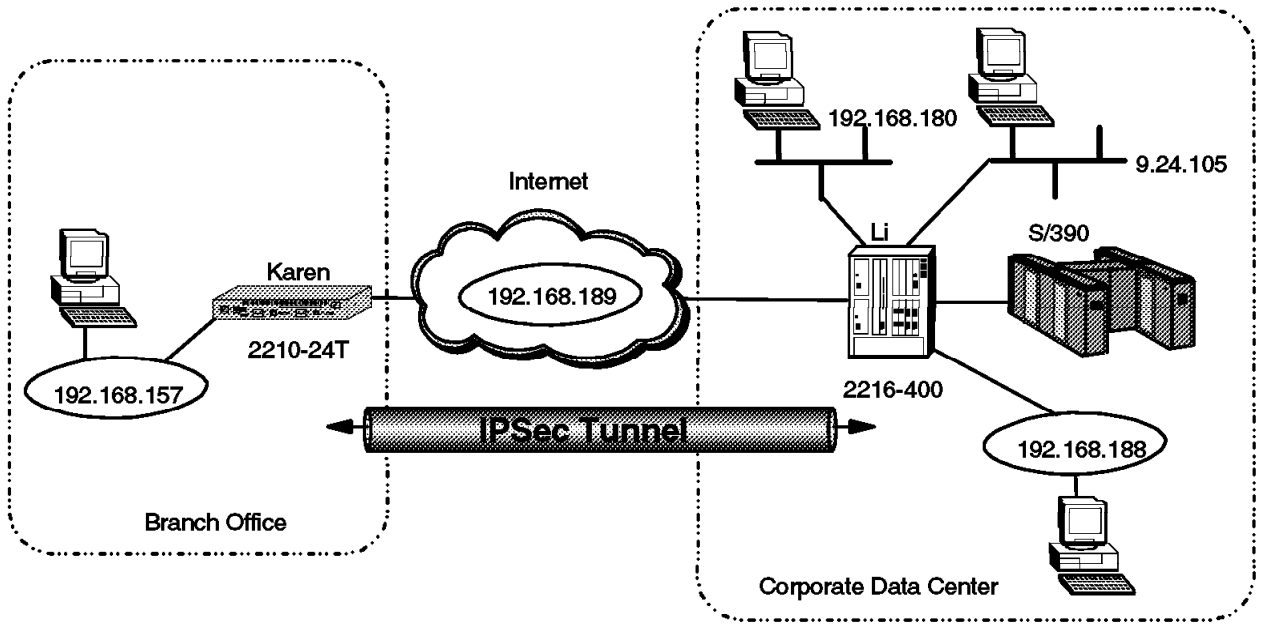


Figure 38. Branch Office Connection with a VPN

Note: In our laboratory environment we used a token-ring LAN as our insecure network. Hereafter, we refer to this insecure network as the “Internet” and to the interfaces of the 2210 and 2216 connected to this network as the “public interfaces.” Most probably, your routers will be connected to the Internet via serial PPP or frame relay connections. This, however, does not change the basic steps to configure the IPSec tunnel between the routers. The routers just need IP connectivity for the tunnels.

The 2216 and 2210 have been named “Li” and “Karen” respectively. These host names are visible in the configuration screens so that you can easily distinguish which commands are for the 2216 and which for the 2210.

For testing purposes, we placed different kinds of clients and servers (FTP, telnet, HTTP, IPX and NetBIOS), APPN(HPR) network nodes, 3270 clients and an OS/390 host in both our intranet and Internet. The OS/390 host was connected to a channel adapter in the 2216 on the main site. In the scenario where we start using the host-connectivity a short example of the configuration of this connection is provided.

As discussed in 2.1.1, “Defining the Router Interfaces” on page 9, the prerequisite for defining an IPSec tunnel is to configure your hardware interfaces, IP addresses and masks on each router interface that will serve as an IPSec tunnel endpoint. Appendix A, “Basic Router Configuration” on page 135 shows the Quick Config screens from when we configured the routers for the scenarios in this redbook.

3.1.1 Configuring the Branch Office Router

In this section, we provide the configuration of the router in the branch office. The configuration of the router in the corporate site is discussed in 3.1.2, “Configuring IPSec at the Data Center” on page 46.

The first step is to create the packet filters on the interface that connects to the Internet (the public interface). This interface will be the endpoint of our IPSec tunnel at the branch office. We need to define two filters: one for out-bound traffic and one for in-bound traffic. We give each filter a name that corresponds to the function of the filter. For example, `pf_in_0` is the packet filter for the inbound traffic on interface 0 of the router. Figure 39 shows the `add packet-filter` commands used to create these filters for our scenario.

```
Karen *t 6
Gateway user configuration
Karen Config>protocol ip
Internet protocol user configuration
Karen IP config>add packet-filter
Packet-filter name []? pf_out_0
Filter incoming or outgoing traffic? [IN]? out
Which interface is this filter for [0]?
Karen IP config>add packet-filter
Packet-filter name []? pf_in_0
Filter incoming or outgoing traffic? [IN]?
Which interface is this filter for [0]?
Karen IP config>
```

Figure 39. Creating the Packet Filter on the Public Interface (0)

Now, we have packet filters created, but we have not specified what criteria will be used to accept or reject packets. These *access controls* are added to the these newly-created packet filters using the update command followed by the add access-control command.

As discussed in 2.1.2, “Packet Filters and IPSec” on page 10, the IPSec access control is used slightly differently between outbound and inbound packet filters. For outbound packet filters, a packet that matches an IPSec (type S) control is indeed sent to the IPSec engine, while for an inbound packet filter, the type S control is used after a packet leaves the IPSec engine and is used to verify the tunnel number.

The access controls in a packet filter will be evaluated on the packets in the order which they are listed. The first control that matches the packet will be executed. Thus, the packet will be accepted if it matches an inclusive control, dropped if it matches an exclusive control or sent to IPSec if it matches an S control. If no access control in the list matches the packet, it is dropped.

The order of the controls in the list is therefore very important. For example, if you add a new access control for a specific host in the Internet to communicate via a tunnel with your site and this access control is in the list after one that excludes any communication for all Internet hosts, then the new access control will never be used. You can use the move access-control command to change positions of the controls in the list and delete access-control to remove a control.

Figure 40 shows the commands to add the first filter criteria for the outbound traffic (the traffic leaving our branch over the IPSec tunnel). This first control is an *IPSec* access control that specifies to funnel all packets with the following criteria to the IPsec engine for further processing:

- Source address of the 192.168.157 subnet in the branch office
- Destination address of the 192.168.180 subnet in the corporate site
- Any IP protocol

```
Karen IP config>update packet-filter pf_out_0
Karen Packet-filter 'pf_out_0' Config>add access-control
Enter type [E]? s
Internet source [0.0.0.0]? 192.168.157.0
Source mask [255.255.255.255]? 255.255.255.0
Internet destination [0.0.0.0]? 192.168.180.0
Destination mask [255.255.255.255]? 255.255.255.0
Enter starting protocol number ([0] for all protocols) [0]?
Enter IPsec Tunnel ID [1]?
Enable Logging(Yes or [No]):
Karen Packet-filter 'pf_out_0' Config>
```

Figure 40. Configuring the Outbound Packet Filter on the Branch Router

The specification of tunnel number one in the access control says that all such traffic will be sent over IPSec tunnel number one. We will configure the tunnel later in this section after the configuration of the packet filters.

It is important to remember that we use a tunnel-mode IPSec tunnel for traffic coming from/going to one of our private subnets. Tunnel mode will hide these

addresses from anyone on the Internet who might be trying to eavesdrop on the communication. Using tunnel mode means that the IPSec engine will encapsulate the original packet in a new IP packet with the IP addresses of the two routers.

After the packet has been processed by IPSec, it is passed back through the IP filters. It will now have an IP protocol number of 50 or 51 (for ESP and AH respectively). Thus we need to configure another access control in the outbound filter with the following criteria:

- A source address of the local side of the IPSec tunnel
- A destination address of the remote side of the IPSec tunnel
- An IP protocol field that indicates it is an IPSec packet (protocol 50-51)

Figure 41 shows the command used to define this control for our scenario.

```
Karen Packet-filter 'pf_out_0' Config>add access-control
Enter type [E]? i
Internet source [0.0.0.0]? 192.168.189.59
Source mask [255.255.255.255]?
Internet destination [0.0.0.0]? 192.168.189.1
Destination mask [255.255.255.255]?
Enter starting protocol number ([0] for all protocols) [0]? 50
Enter ending protocol number [50]? 51
Enable Logging(Yes or [No]):
Karen Packet-filter 'pf_out_0' Config>
```

Figure 41. Configuring the Outbound Packet Filter on the Branch Router

Later in our scenario, we create several configurations that involve router-to-router traffic that we also need to secure via IPSec. These include:

- Data Link Switching (DLSw)
- An IP bridging tunnel
- Enterprise Extender (HPR over IP)

With these types of traffic, you could either use tunnel-mode or transport-mode tunnels. Technically, with these types of traffic, the routers act as IP hosts. It is common practice to use transport-mode tunnels for host-to-host traffic because there is no need to camouflage the IP addresses in the original IP headers as is done with tunnel mode.

However, it is not required to use a transport-mode tunnel for router-to-router communication. We could use the same tunnel-mode tunnel that we use for communication between the intranet LAN's.

There are trade-offs either way. If you use the existing tunnel-mode tunnel, you will create larger IP packets than is strictly necessary, since you add an IP header and trailer. On the other hand you keep your tunnel database smaller, thus reducing processing by the router. So you have to make a trade off between more overhead in your traffic (you will use more bandwidth) or more processing in your router (you will consume slightly more DRAM and processing power).

In our scenario, we chose a separate transport-mode tunnel for the router-to-router communication, since we only have two sites to connect to each

other. Therefore, the next step is to add another access control of type S (IPSec) that is used to funnel the router-to-router traffic to IPSec for processing. The control will have the following criteria:

- Source address of the local router's internal address
- Destination address of the remote router's internal address
- All IP protocols are allowed

Figure 42 shows the commands used to define this control for our scenario.

```
Karen Packet-filter 'pf_out_0' Config>add access-control
Enter type [E]? s
Internet source [0.0.0.0]? 192.168.189.59
Source mask [255.255.255.255]?
Internet destination [0.0.0.0]? 192.168.189.1
Destination mask [255.255.255.255]?
Enter starting protocol number ([0] for all protocols) [0]?
Enter IPsec Tunnel ID [1]? 2
Enable Logging(Yes or [No]):
Karen Packet-filter 'pf_out_0' Config>
```

Figure 42. Configuring the Outbound Packet Filter on the Branch Router

Since we chose to use a transport-mode tunnel, this is a different tunnel than the one we use to send the intranet traffic and so we specify a new tunnel ID (tunnel number 2) for this traffic. This tunnel is defined later in this scenario in 3.1.1.4, "Defining the IPSec Tunnels" on page 42.

Next, we list the access controls for this packet filter. Figure 43 shows this listing for our scenario.

```
Karen Packet-filter 'pf_out_0' Config>list access-control
Access Control is: disabled
Access Control facility: USER

List of access control records:

1   Type=I S   Source=192.168.157.0    Dest=192.168.180.0    Prot=  0-255
               Mask=  255.255.255.0    Mask=255.255.255.0
               SPorts=N/A              DPorts=N/A            Tid=1
                                       Log=No

2   Type=I     Source=192.168.189.59   Dest=192.168.189.1    Prot= 50-51
               Mask=  255.255.255.255  Mask=255.255.255.255
               SPorts=    0-65535      DPorts=    0-65535
                                       Log=No

3   Type=I S   Source=192.168.189.59   Dest=192.168.189.1    Prot=  0-255
               Mask=  255.255.255.255  Mask=255.255.255.255
               SPorts=N/A              DPorts=N/A            Tid=2
                                       Log=No
Karen Packet-filter 'pf_out_0' Config>exit
Karen IP config>
```

Figure 43. Listing the Access Controls

Important Note

The position of the access controls is very critical here, especially the controls that specify the router-to-router IP addresses (controls 2 and 3). We have placed the most specific control (protocols 50-51) in front of the more generic control (all protocols). It has to be this way or the tunnel-mode IPSec packets will never leave the box.

The transport-mode packets (HPR/IP packets for example) will not match access control number 2 but will match control number 3. They will get passed to IPSec for processing and then passed back through the filters where they will match control number 2 since they will then have a protocol field of 50 or 51.

This completes the definition of the packet filter for the outbound traffic.

3.1.1.1 Defining the Inbound Packet Filters

Next, we need to add the access controls for the inbound traffic. Now that we have configured the outbound packet filter we understand what kinds of packets we can expect on the inbound traffic via the public interface. To start with, we will receive IPSec traffic from the other router; thus the first control is an *inclusive* control that specifies to accept all packets with the following criteria:

- A source address of the remote side of the IPSec tunnel
- A destination address of the local side of the IPSec tunnel
- An IP protocol field that indicates it is an IPSec packet (protocol 50-51)

Figure 44 shows the commands to add this access control.

```
Karen IP config>update packet-filter pf_in_0
Karen Packet-filter 'pf_in_0' Config>add access-control
Enter type [E]? i
Internet source [0.0.0.0]? 192.168.189.1
Source mask [255.255.255.255]?
Internet destination [0.0.0.0]? 192.168.189.59
Destination mask [255.255.255.255]?
Enter starting protocol number ([0] for all protocols) [0]? 50
Enter ending protocol number [50]? 51
Enable Logging(Yes or [No]):
Karen Packet-filter 'pf_in_0' Config>
```

Figure 44. Configuring the Inbound Packet Filter on the Branch Router

Any packet that matches the criteria in the first filter gets passed to the IPSec engine in the router since this engine takes care of all traffic that is sent to the router with IP protocol 50 or 51.

Next, we add the access control that will accept traffic from the intranet segment(s) located at the central site. In this case, we specify that any packet from the 192.168.180 subnetwork that is destined for the 192.168.157 subnetwork should be allowed into our router. Thus the control has the following criteria:

- The source is the 192.168.180 subnet in the corporate site
- The destination is the 192.168.157 subnet in the branch office
- All IP protocols are allowed

This is an S type control and we specify to use tunnel number 1 for this traffic. Figure 45 on page 39 shows the commands used for our scenario.

```
Karen Packet-filter 'pf_in_0' Config>add access-control
Enter type [E]? s
Internet source [0.0.0.0]? 192.168.180.0
Source mask [255.255.255.255]? 255.255.255.0
Internet destination [0.0.0.0]? 192.168.157.0
Destination mask [255.255.255.255]? 255.255.255.0
Enter starting protocol number ([0] for all protocols) [0]?
Enter IPsec Tunnel ID [1]?
Enable Logging(Yes or [No]):
Karen Packet-filter 'pf_in_0' Config>
```

Figure 45. Configuring the Inbound Packet Filter on the Branch Router

The next access control that we need for in-bound traffic for this interface is for the router-to-router traffic via the transport-mode tunnel. The control for this traffic has the following criteria:

- An S type control using tunnel number 2
- The source address is the remote router's internal address
- The destination address is the local router's internal address
- All IP protocols are allowed

Figure 46 shows the commands used to add this access control.

```
Karen Packet-filter 'pf_in_0' Config>add access-control
Enter type [E]? s
Internet source [0.0.0.0]? 192.168.189.1
Source mask [255.255.255.255]?
Internet destination [0.0.0.0]? 192.168.189.59
Destination mask [255.255.255.255]?
Enter starting protocol number ([0] for all protocols) [0]?
Enter IPsec Tunnel ID [1]? 2
Enable Logging(Yes or [No]):
Karen Packet-filter 'pf_in_0' Config>
```

Figure 46. Configuring the Inbound Packet Filter on the Branch Router

Next, we list the access controls for this packet filter. Figure 47 on page 40 shows the listing for our scenario.

```
Karen Packet-filter 'pf_in_0' Config>list access-control
Access Control is: disabled
Access Control facility: USER

List of access control records:

1   Type=I     Source=192.168.189.1    Dest=192.168.189.59   Prot= 50-51
               Mask=  255.255.255.255  Mask=255.255.255.255
               SPorts=    0-65535      DPorts=    0-65535
                                       Log=No

2   Type=I S   Source=192.168.180.0    Dest=192.168.157.0    Prot=  0-255
               Mask=  255.255.255.0    Mask=255.255.255.0
               SPorts=N/A              DPorts=N/A            Tid=1
                                       Log=No

3   Type=I S   Source=192.168.189.1    Dest=192.168.189.59   Prot=  0-255
               Mask=  255.255.255.255  Mask=255.255.255.255
               SPorts=N/A              DPorts=N/A            Tid=2
                                       Log=No
Karen Packet-filter 'pf_in_0' Config>exit
Karen IP config>
```

Figure 47. Listing Access Controls on the Inbound Packet Filter

This completes the definition of the packet filters for the inbound traffic from the 192.168.180 subnet pictured in Figure 38 on page 33.

3.1.1.2 Configuring Additional Subnets

To permit more subnets or hosts to use our tunnel-mode tunnel, we just need to add access controls of type *S* for the other combinations of source and destination hosts or subnets that need communication across the IPSec tunnel. Remember that we need an additional access control on both the inbound and outbound filters similar to those depicted in Figure 40 on page 35 and Figure 45 on page 39.

In this section, we add additional access controls in the inbound and outbound packet filters for communication between the other Ethernet LAN (the 9.24.105 subnet) in the corporate site and the token-ring LAN in the branch office. Figure 48 on page 41 and Figure 49 on page 41 show the commands to add the controls and to move them just after the other access controls for communication between the intranet LAN's.

```
Karen IP config>update packet-filter pf_out_0
Karen Packet-filter 'pf_out_0' Config>add access-control
Enter type [E]? s
Internet source [0.0.0.0]? 192.168.157.0
Source mask [255.255.255.255]? 255.255.255.0
Internet destination [0.0.0.0]? 9.24.105.0
Destination mask [255.255.255.255]? 255.255.255.0
Enter starting protocol number ([0] for all protocols) [0]?
Enter IPsec Tunnel ID [1]?
Enable Logging(Yes or [No]):
Karen Packet-filter 'pf_out_0' Config>move access-control 4 1
About to move:

4   Type=I S   Source=192.168.157.0    Dest=9.24.105.0       Prot=  0-255
               Mask=  255.255.255.0    Mask=255.255.255.0
               SPorts=N/A              DPorts=N/A            Tid=1
                                       Log=No
to be after:

1   Type=I S   Source=192.168.157.0    Dest=192.168.180.0    Prot=  0-255
               Mask=  255.255.255.0    Mask=255.255.255.0
               SPorts=N/A              DPorts=N/A            Tid=1
                                       Log=No
Are you sure this is what you want to do(Yes or [No]): yes
Karen Packet-filter 'pf_out_0' Config>exit
Karen IP config>
```

Figure 48. Adding and Moving an Access Control for the Outbound Packet Filter

```
Karen IP config>update packet-filter pf_in_0
Karen Packet-filter 'pf_in_0' Config>add access-control
Enter type [E]? s
Internet source [0.0.0.0]? 9.24.105.0
Source mask [255.255.255.255]? 255.255.255.0
Internet destination [0.0.0.0]? 192.168.157.0
Destination mask [255.255.255.255]? 255.255.255.0
Enter starting protocol number ([0] for all protocols) [0]?
Enter IPsec Tunnel ID [1]?
Enable Logging(Yes or [No]):
Karen Packet-filter 'pf_in_0' Config>move access-control 4 2
About to move:

4   Type=I S   Source=9.24.105.0       Dest=192.168.157.0    Prot=  0-255
               Mask=  255.255.255.0    Mask=255.255.255.0
               SPorts=N/A              DPorts=N/A            Tid=1
                                       Log=No
to be after:

2   Type=I S   Source=192.168.180.0    Dest=192.168.157.0    Prot=  0-255
               Mask=  255.255.255.0    Mask=255.255.255.0
               SPorts=N/A              DPorts=N/A            Tid=1
                                       Log=No
Are you sure this is what you want to do(Yes or [No]): yes
Karen Packet-filter 'pf_in_0' Config>exit
Karen IP config>
```

Figure 49. Adding and Moving an Access Control for the Inbound Packet Filter

3.1.1.3 Enabling Access Control and the Packet Filters

At this point, the packet filters and their corresponding access controls have been defined. However, they are not active until we globally enable access control on the router.

Figure 50 shows the command to enable access control at the box level. The list command is used to verify that access control has been enabled for the router.

Note: In addition to enabling access control at the box level, you can also enable/disable each packet filter individually. (The default state at creation time is enabled.) The list command also shows the state of each packet filter.

```
Karen IP config>set access-control on
Karen IP config>list packet-filter

List of packet-filter records:

Name               Direction   Interface   State  Src-Addr-Ver
pf_in_0            In          0           On     Off
pf_out_0           Out         0           On     N/A
Access Control is: enabled
Karen IP config>exit
```

Figure 50. Enabling Access Controls

3.1.1.4 Defining the IPSec Tunnels

At this point, we have the correct packet filters and access controls defined and enabled but we have not yet defined the IPSec tunnels. The next few figures show the definition of the first tunnel.

Figure 51 on page 43 shows that a tunnel is defined from within the IPSec feature of the Talk 6 menus. The `add tunnel` command is used to create the tunnel and after this command you are prompted for all variables you need to set.

The first tunnel we create will be a tunnel-mode tunnel with id=1 and we have chosen to use AH-ESP as tunnel policy. As discussed in 2.1.5, “Defining the IPSec Tunnel” on page 19, AH_ESP is the choice if you want to perform encryption and authorization using both the IPSec ESP and AH protocols. This selection indicates that for packets in the outbound direction, the packets will be encrypted first via the ESP protocol, then the AH algorithms will be run on the encrypted payload. We have chosen to use AH_ESP because we want both authentication and encryption to run. Also, we want the more complete authentication provided by the AH protocol which authenticates the complete packet, including the ESP and IP headers.

```
Karen Config>feature ipsec
IP Security feature user configuration
Karen IPsec config>add tunnel
Tunnel ID (1-65535) [1]?
Tunnel Name (optional) []? ESP&AH1
Tunnel Lifetime, in minutes (0-525600) [46080]?
Tunnel Encapsulation Mode (TUNN or TRANS) [TUNN]?
Tunnel Policy (AH,ESP,AH-ESP,ESP-AH) [AH-ESP]?
```

Figure 51. Defining the Tunnel-Mode IPSec Tunnel on the Branch Router

Next, we are prompted to define the *local end* of the Security Association (SA). Figure 52 shows the required parameters. The local algorithms are used on the outbound packets and the remote algorithms are used on the inbound packets. We input all SPIs to a value of 256, the AH algorithm is HMAC-MD5 and the Encryption algorithm is DES-CBC.

The local SPIs are the SPIs expected in inbound packets, and the remote SPIs are placed in the outbound packets. To prevent problems with remote and local SPIs and algorithms we advise you to use the same SPIs and algorithms on both sides.

It cannot be stressed enough that since your routers are connected to the Internet you have to take all measures within your ability to make them secure. Use strict rules which the keys must satisfy just as you probably have for passwords in your systems and networks. For example, change them periodically, use alphanumeric characters, and do not use a convention for creating your passwords (like using the IP address and/or host name in the key).

```
Local IP Address [192.168.189.59]?
Local Authentication SPI (256-65535) [256]?
Local Authentication Algorithm (HMAC-MD5,HMAC-SHA) [HMAC-MD5]?
Local Authentication Key (32 characters) in Hex (0-9,a-f,A-F):
Enter Local Authentication Key again (32 characters) in Hex (0-9,a-f,A-F):
Local Encryption SPI (256-65535) [256]?
Local Encryption Algorithm (DES-CBC,CDMF,3DES) [DES-CBC]?
Local Encryption Key (16 characters) in Hex (0-9,a-f,A-F):
Enter Local Encryption Key again (16 characters) in Hex (0-9,a-f,A-F):
Additional Padding for Local Encryption (0-120) [0]?
Do you wish to use local ESP authentication? [No]:
```

Figure 52. Defining the Tunnel-Mode IPSec Tunnel on the Branch Router

Note: The keys are not displayed while typed.

Next, we are prompted to define the *remote end* of the SA. Figure 53 on page 44 shows the required parameters.

```
Remote IP Address [0.0.0.0]? 192.168.189.1
Remote Authentication SPI (1-65535) [256]?
Remote Authentication Algorithm (HMAC-MD5,HMAC-SHA) [HMAC-MD5]?
Remote Authentication Key (32 characters) in Hex (0-9,a-f,A-F):
Enter Remote Authentication Key again (32 characters) in Hex (0-9,a-f,A-F):
Remote Encryption SPI (1-65535) [256]?
Remote Encryption Algorithm (DES-CBC,CDMF,3DES) [DES-CBC]?
Remote Encryption Key (16 characters) in Hex (0-9,a-f,A-F):
Enter Remote Encryption Key again (16 characters) in Hex (0-9,a-f,A-F):
Do you wish to perform verification of remote encryption padding? [No]:
Do you wish to use remote ESP authentication? [No]:
Enable replay prevention? [No]:
Do you wish to enable this tunnel? [Yes]:
Karen IPsec config>
```

Figure 53. Defining the Tunnel-Mode IPSec Tunnel on the Branch Router

The next tunnel we create is the transport-mode tunnel for the router-to-router traffic. We specify an id of 2 for this tunnel and we use AH-ESP again as the tunnel policy. The value of 257 is used for the SPIs, the AH algorithm is HMAC-MD5, and the 3DES algorithm is used for encryption. Figure 54, Figure 55 on page 45, and Figure 56 on page 45 show the configuration of this transport-mode tunnel.

```
Karen IPsec config>add tunnel
Tunnel ID (1-65535) [1]? 2
Tunnel Name (optional) []? TRANS-ESP&AH
Tunnel Lifetime, in minutes (0-525600) [46080]?
Tunnel Encapsulation Mode (TUNN or TRANS) [TUNN]? TRANS
Tunnel Policy (AH,ESP,AH-ESP,ESP-AH) [AH-ESP]?
```

Figure 54. Defining the Transport-Mode IPSec Tunnel on the Branch Router

Next, we are prompted to define the local end of the SA. Figure 55 on page 45 shows the required parameters.

```
Local IP Address [192.168.189.59]?
Local Authentication SPI (256-65535) [256]? 257
Local Authentication Algorithm (HMAC-MD5,HMAC-SHA) [HMAC-MD5]?
Local Authentication Key (32 characters) in Hex (0-9,a-f,A-F):
Enter Local Authentication Key again (32 characters) in Hex (0-9,a-f,A-F):
Local Encryption SPI (256-65535) [257]?
Local Encryption Algorithm (DES-CBC,CDMF,3DES) [DES-CBC]? 3DES
First Local Encryption Key (16 characters) in Hex (0-9,a-f,A-F):
Enter First Local Encryption Key again (16 characters) in Hex (0-9,a-f,A-F):
Second Local Encryption Key (16 characters) in Hex (0-9,a-f,A-F):
Enter Second Local Encryption Key again (16 characters) in Hex (0-9,a-f,A-F):
Third Local Encryption Key (16 characters) in Hex (0-9,a-f,A-F):
Enter Third Local Encryption Key again (16 characters) in Hex (0-9,a-f,A-F):
Additional Padding for Local Encryption (0-120) [0]?
Do you wish to use local ESP authentication? [No]:
```

Figure 55. Defining the Transport-Mode IPSec Tunnel on the Branch Router

Next, we are prompted to define the remote end of the SA. Figure 56 shows the required parameters.

```
Remote IP Address [0.0.0.0]? 192.168.189.1
Remote Authentication SPI (1-65535) [257]?
Remote Authentication Algorithm (HMAC-MD5,HMAC-SHA) [HMAC-MD5]?
Remote Authentication Key (32 characters) in Hex (0-9,a-f,A-F):
Enter Remote Authentication Key again (32 characters) in Hex (0-9,a-f,A-F):
Remote Encryption SPI (1-65535) [257]?
Remote Encryption Algorithm (DES-CBC,CDMF,3DES) [3DES]?
First Remote Encryption Key (16 characters) in Hex (0-9,a-f,A-F):
Enter First Remote Encryption Key again (16 characters) in Hex (0-9,a-f,A-F):
Second Remote Encryption Key (16 characters) in Hex (0-9,a-f,A-F):
Enter Second Remote Encryption Key again (16 characters) in Hex (0-9,a-f,A-F):
Third Remote Encryption Key (16 characters) in Hex (0-9,a-f,A-F):
Enter Third Remote Encryption Key again (16 characters) in Hex (0-9,a-f,A-F):
Do you wish to perform verification of remote encryption padding? [No]:
Do you wish to use remote ESP authentication? [No]:
Enable replay prevention? [No]:
Do you wish to enable this tunnel? [Yes]:
Karen IPsec config>
```

Figure 56. Defining the Transport-Mode IPSec Tunnel on the Branch Router

Next, we list the tunnels that we have created. Figure 57 on page 46 shows the command and output.

```
Karen IPsec config>list tunnel all

   ID         Name          Local IP Addr   Remote IP Addr   Mode    State
 ------  ---------------  ---------------  ---------------  -----  --------
      2  TRANS-ESP&AH     192.168.189.59   192.168.189.1    TRANS  Enabled
      1  ESPAH            192.168.189.59   192.168.189.1    TUNN   Enabled
Karen IPsec config>
```

Figure 57. Listing Defined Tunnels on the Branch Router

The last step is to enable IPSec on the router. Figure 58 shows this command.

```
Karen IPsec config>enable ipsec
Restarting the router is required for IPsec to be active.
Karen IPsec config>exit
Karen Config>
```

Figure 58. Enabling IPSec

As the message from the router indicates, we need to restart the router so that the newly created IPSec tunnel will be activated.

```
Karen Config> <CTRL>+<P>
Karen *restart
Are you sure you want to restart the gateway? (Yes or [No]): yes
```

Figure 59. Restarting the Router

3.1.2 Configuring IPSec at the Data Center

Now we need to perform the same steps to configure the router Li at the corporate data center. The only differences are:

- The IP addresses in the filters and the tunnels will be swapped from those that we used for the branch router configuration.
- The parameters in the tunnel definitions will also be swapped. The values used for the remote end at the branch router are now the ones used for the local end at the data center router and vice versa. (However, for the most part, we used the same values for both the remote and the local end, so this is not a very big issue.)

For completeness, these screens are documented in Appendix B, “Configuring the IPSec Tunnels at the Data Center” on page 149.

3.2 Monitoring and Troubleshooting

In this section, we show a couple of useful commands to display statistics about the state and the use of tunnels and the packet filters. We only show the commands on the 2216 in our scenario. However, the commands and outputs on an IBM 2210 are exactly the same.

The first thing to check after the routers have been restarted with the new IPSec configuration is to make sure that you still have IP connectivity to the other side of the tunnel. In Figure 60, you can see a ping command from the IP prompt in Talk 5 where nine pings from router Li to router Karen were sent.

```
MOS Operator Control

Li * t 5

Li IP>ping 192.168.189.59
PING 192.168.189.1 -> 192.168.189.59: 56 data bytes, ttl=64, every 1 sec.
56 data bytes from 192.168.189.59: icmp_seq=0. ttl=64. time=0. ms
56 data bytes from 192.168.189.59: icmp_seq=1. ttl=64. time=0. ms
56 data bytes from 192.168.189.59: icmp_seq=2. ttl=64. time=0. ms
56 data bytes from 192.168.189.59: icmp_seq=3. ttl=64. time=0. ms
56 data bytes from 192.168.189.59: icmp_seq=4. ttl=64. time=0. ms
56 data bytes from 192.168.189.59: icmp_seq=5. ttl=64. time=0. ms
56 data bytes from 192.168.189.59: icmp_seq=6. ttl=64. time=0. ms
56 data bytes from 192.168.189.59: icmp_seq=7. ttl=64. time=0. ms
56 data bytes from 192.168.189.59: icmp_seq=8. ttl=64. time=0. ms

----192.168.189.59 PING Statistics----
9 packets transmitted, 9 packets received, 0% packet loss
round-trip min/avg/max = 0/0/0 ms
Li IP>
```

Figure 60. Pinging the Other Side of the Tunnel

In addition, we issued four pings from a station in the 9.24.105 subnet on the corporate site to a station in the 192.168.157 subnet in the branch office (not shown) to check end-to-end connectivity between the branch and the data center.

These pings not only check the connectivity through our tunnel, but they also generate some traffic that we can use to check our access controls to see how many packets matched each control. We look at the number for “use” in the last column of the output which tells us the number of times that the access control has been matched.

Figure 61 on page 48 shows the command and output for the outbound packet filter and you can see that access control number 2 was matched 4 times which correlates to the 4 pings between the two intranet LANs. Control number 4 was matched nine times which correlates to the nine pings between the routers. And since all pings are sent via an IPSec tunnel, we also see 13 matches for control number 3 for IPSec packets that are sent to the other router.

```
Li IP>packet-filter pf_out_0
Name              Dir  Intf  State  Src-Addr-Ver  #Access-Controls
pf_out_0          Out  0     On     N/A           4

Access Control currently enabled
Access Control facility: USER

Access Control run 165 times, 327 cache hits

List of access control records:

1   Type=I S   Source=192.168.180.0    Dest=192.168.157.0    Prot=  0-255
               Mask=  255.255.255.0    Mask=255.255.255.0    Use=0
               SPorts=N/A              DPorts=N/A            Tid=1
                                       Log=No

2   Type=I S   Source=9.24.105.0       Dest=192.168.157.0    Prot=  0-255
               Mask=  255.255.255.0    Mask=255.255.255.0    Use=4
               SPorts=N/A              DPorts=N/A            Tid=1
                                       Log=No

3   Type=I     Source=192.168.189.1    Dest=192.168.189.59   Prot= 50-51
               Mask=  255.255.255.255  Mask=255.255.255.255  Use=13
               SPorts=    0-65535      DPorts=    0-65535
                                       Log=No

4   Type=I S   Source=192.168.189.1    Dest=192.168.189.59   Prot=  0-255
               Mask=  255.255.255.255  Mask=255.255.255.255  Use=9
               SPorts=N/A              DPorts=N/A            Tid=2
                                       Log=No
Li IP>
```

Figure 61. Showing the Outbound Packet Filter

Figure 62 on page 49 shows the command for displaying the statistics of the inbound packet filter. Here we see similar statistics that have resulted from the packets that were echoed from the other router.

Note that access control number 1 is matched twice for each IPSec packet that enters the router from our ping command. This is a result of the way in which packets flow in the router. Tunnel-mode IPSec packets are matched twice because the access controls are checked just after the packet enters the interface and again after the destination is determined to be for the local queue (the router itself is the destination). Finally, in the case of the router-to-router pings, after the packet is decapsulated in the IPSec engine, it is passed through the filters again where it matches access control number 4. See 2.1.2, “Packet Filters and IPSec” on page 10 for more information about the internal packet flow in the router.

```
Li IP>packet-filter pf_in_0
Name              Dir  Intf  State  Src-Addr-Ver  #Access-Controls
pf_in_0           In   0     On     Off           4

Access Control currently enabled
Access Control facility: USER

Access Control run 507 times, 875 cache hits

List of access control records:

1   Type=I     Source=192.168.189.59   Dest=192.168.189.1    Prot= 50-51
               Mask=  255.255.255.255  Mask=255.255.255.255  Use=26
               SPorts=    0-65535      DPorts=    0-65535
                                       Log=No

2   Type=I S   Source=192.168.157.0    Dest=192.168.180.0    Prot=  0-255
               Mask=  255.255.255.0    Mask=255.255.255.0    Use=0
               SPorts=N/A              DPorts=N/A            Tid=1
                                       Log=No

3   Type=I S   Source=192.168.157.0    Dest=9.24.105.0       Prot=  0-255
               Mask=  255.255.255.0    Mask=255.255.255.0    Use=4
               SPorts=N/A              DPorts=N/A            Tid=1
                                       Log=No

4   Type=I S   Source=192.168.189.59   Dest=192.168.189.1    Prot=  0-255
               Mask=  255.255.255.255  Mask=255.255.255.255  Use=9
               SPorts=N/A              DPorts=N/A            Tid=2
                                       Log=No
Li IP>exit
Li +
```

Figure 62. Showing the Inbound Packet Filter

Other useful information regarding the IPSec tunnels can be obtained from the IPSec prompt in Talk 5. In Figure 63 on page 50, Figure 64 on page 50, and Figure 65 on page 51 we show several variations of the `list` command:

- `List global` displays the state of IPSec (enabled/disabled)
- `List all` displays the defined and active tunnels with details
- `List tunnel active` and `list tunnel defined` display more details about active and defined tunnels

```
Li +feature ipsec
Li IPsec>list global

IPsec is ENABLED
Li IPsec>list all

IPsec is ENABLED

Defined Manual Tunnels:

   ID         Name         Local IP Addr   Remote IP Addr   Mode    State
 ------  ---------------  ---------------  ---------------  -----  --------
      1  ESP&AH             192.168.189.1   192.168.189.59  TUNN   Enabled
      2  TRANS-ESP&AH       192.168.189.1   192.168.189.59  TRANS  Enabled

Tunnel Cache:

 ID     Local IP Addr   Remote IP Addr   Mode   Policy  Tunnel Expiration
-----  ---------------  ---------------  -----  ------  ------------------
    2    192.168.189.1   192.168.189.59  TRANS  AH-ESP  16:47  Jun 20 1998
    1    192.168.189.1   192.168.189.59  TUNN   AH-ESP  16:47  Jun 20 1998
Li IPsec>
```

Figure 63. Listing IPSec Information

```
Li IPsec>list tunnel active


Tunnel       Name        Mode   Policy   Life   Replay        Tunnel
  ID                                             Prev       Expiration
------  ---------------  -----  ------  ------  ------  ------------------
     1  ESP&AH           TUNN   AH-ESP   46080    No    17:18  Jun 20 1998

Local Information:

      IP Address: 192.168.189.1
  Authentication:  SPI:   256    Algorithm: HMAC-MD5
      Encryption:  SPI:   256    Encryption Algorithm: DES-CBC
                                 Extra Pad:   0
                                 ESP Authentication Algorithm: ----------
Remote Information:

      IP Address: 192.168.189.59
  Authentication:  SPI:   256    Algorithm: HMAC-MD5
      Encryption:  SPI:   256    Encryption Algorithm: DES-CBC
                                 Verify Pad?:  No
                                 ESP Authentication Algorithm: ----------
```

Figure 64. Listing Active Tunnels

```
Li IPsec>list tunnel defined
Enter the Tunnel ID, Tunnel Name, or 'ALL' [ALL]? 2

Tunnel        Name         Mode    Policy    Life    Replay    State
  ID                                                 Prev
------   --------------   -----   ------   ------   ------   --------
     2   TRANS-ESP&AH      TRANS   AH-ESP    46080     No     Enabled

Local Information:

      IP Address: 192.168.189.1
  Authentication:  SPI:   257    Algorithm: HMAC-MD5
      Encryption:  SPI:   257    Encryption Algorithm: 3DES
                                 Extra Pad:   0
                                 ESP Authentication Algorithm: ----------
Remote Information:

      IP Address: 192.168.189.59
  Authentication:  SPI:   257    Algorithm: HMAC-MD5
      Encryption:  SPI:   257    Encryption Algorithm: 3DES
                                 Verify Pad?:  No
                                 ESP Authentication Algorithm: ----------
Li IPsec>
```

Figure 65. Listing Defined Tunnels

Another useful command from the IPSec prompt in Talk 5 is the stats command. This command gives some statistics about the packets handled by IPSec. Figure 66 on page 52 and Figure 67 on page 52 give the statistics for tunnel 1 and tunnel 2 respectively. In these, you can also see the 4 pings between the two intranet LAN's over tunnel 1 and the 9 pings between the routers over tunnel 2.

```
Li IPsec>stats
Enter the Tunnel ID, Tunnel Name, or 'ALL' [ALL]? 1

                     Statistics For Secure Tunnel 1
Received:
  total pkts   AH packets   ESP packets   total bytes    AH bytes     ESP bytes
  ----------   ----------   -----------   -----------   ----------   ----------
           8            4             4           896          496          400

Sent:
  total pkts   AH packets   ESP packets   total bytes    AH bytes     ESP bytes
  ----------   ----------   -----------   -----------   ----------   ----------
           8            4             4           752          496          256

Receive Packet Errors:
   AH errors   AH bad seq   ESP errors   ESP bad seq
  ----------   ----------   ----------   -----------
           0            0            0             0

                                                      Send Packet Errors:
   AH errors   ESP errors
  ----------   ----------
           0            0

Li IPsec>
```

Figure 66. Showing IPSec Statistics for Tunnel 1

```
Li IPsec>stats
Enter the Tunnel ID, Tunnel Name, or 'ALL' [ALL]? 2

                     Statistics For Secure Tunnel 2
Received:
  total pkts   AH packets   ESP packets   total bytes    AH bytes     ESP bytes
  ----------   ----------   -----------   -----------   ----------   ----------
          18            9             9          2160         1188          972

Sent:
  total pkts   AH packets   ESP packets   total bytes    AH bytes     ESP bytes
  ----------   ----------   -----------   -----------   ----------   ----------
          18            9             9          2016         1188          828

Receive Packet Errors:
   AH errors   AH bad seq   ESP errors   ESP bad seq
  ----------   ----------   ----------   -----------
           0            0            0             0

                                                      Send Packet Errors:
   AH errors   ESP errors
  ----------   ----------
           0            0

Li IPsec>
```

Figure 67. Showing IPSec Statistics for Tunnel 2

Chapter 4. Data Link Switching over IPSec

Now that the IPSec tunnel is in place between the branch and the data center, we have the capability to securely route IP traffic between these two locations over our virtual private network. However, most enterprise environments today are not IP only networks. Therefore, in order to get the maximum utility of the tunnel, we need to add support for other protocols like SNA and NetBIOS.

DLSw is an IBM-invented standard technology for transporting connection-oriented protocols, mainly SNA and NetBIOS, across IP backbone networks. DLSw routers on the edges of an IP network process link establishment requests from native SNA and NetBIOS end stations, search among peer DLSw routers for one serving the target end station, then set up a path and relay application data between the end stations through the peer router.

With an IPSec tunnel defined between the routers, we can easily define a DLSw connection that uses this tunnel. This chapter describes the procedures for implementing a DLSw connection in a VPN environment using the IBM Nways 2210/2216 routers.

Note

This chapter assumes you are already familiar with DLSw. For more information on using DLSw, please see *IBM 2210 Nways Multiprotocol Router IBM 2216 Nways Multiaccess Connector Description and Configuration Scenarios Volume II*, SG24-4956.

4.1 Configuring DLSw in an IPSec Environment

We use the same configuration here as in Chapter 3, “Connecting the Data Center to the Branch Office” on page 33. We simply build on it to add the DLSw capability. Figure 68 on page 54 shows the network along with the DLSw related parameters.

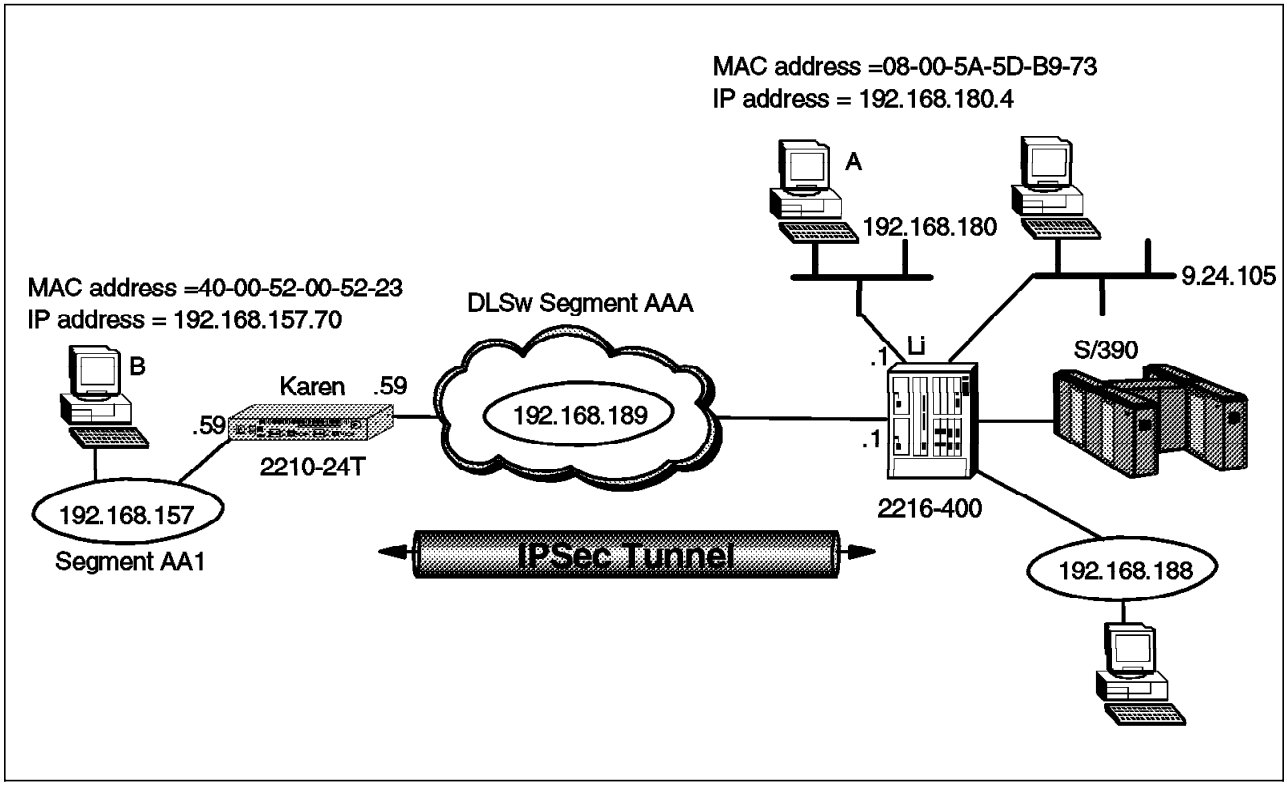


Figure 68. Data Link Switching through an IPSec Tunnel

In order to configure DLSw in the VPN environment, we perform the following procedures:

1. Disable access control
2. Disable IPSec
3. Configure bridging
4. Configure DLSw
5. Enable access control
6. Enable IPSec

Each of these steps is explained in detail in the following sections.

4.1.1 Configuring the Data Center Router

As a first step in adding DLSw to our configuration, we temporarily disable IPSec and access control. This allows us to define and test the DLSw configuration independently of any IPSec functions. After the DLSw configuration is working, we re-enable access control and IPSec.

Note: We recommend that you do this first in order to facilitate any problem determination that may be necessary while bringing up DLSw. Otherwise, if you do experience problems, it will be difficult for you to determine if the problem is in the DLSw configuration or if there is an IPSec problem such as a filter definition.

Figure 69 on page 55 shows the command used to disable access control. As can be seen from the figure, this command is executed from within the IP configuration in the talk 6 process.

Note: Figure 69 on page 55 also illustrates that after you disable access control, you must reset IP in order to make this change effective.

```
Li *t 6
Li Config>p ip
Internet protocol user configuration

Li IP config>set access-control off
Li IP config>exit
Li Config>
Li *t 5
Li +p ip
Li IP>reset ip
Li IP>exit
```

Figure 69. Temporarily Disabling Access Control

Figure 70 shows the command to temporarily disable IPSec on the router. As shown in the figure, this is performed from within the IPSec feature configuration under talk 6.

Note: You can also disable IPSec from the talk 5 process, but like other changes made from talk 5, if you reload the router, this change will be lost and the IPSec function will be enabled when the router comes back up.

```
Li *t 6
Li Config>feature ip
IP Security feature user configuration
Li IPsec config>disable ipsec pass
Li IPsec config>exit
Li Config>
Li *
```

Figure 70. Temporarily Disabling IPSec

Now we configure the bridging function. Here we disable the ports that we are not using in this configuration. For more information on configuring bridging, please see *IBM 2210 Nways Multiprotocol Router Description and Configuration Scenarios Volume I*, SG24-4446.

```
Li Config>p asrt
Adaptive Source Routing Transparent Bridge user configuration
Li ASRT config>ena bridge
Li ASRT config>ena dls
Li ASRT config>disa trans 1
Li ASRT config>disa trans 2
Li ASRT config>disa trans 3
```

Figure 71. Configuring ASRT on the Data Center Router

Now we list the bridge configuration back out to verify that we made the correct changes. This is shown in Figure 72 on page 56.

```
Li ASRT config>list bridge
          Source Routing Transparent Bridge Configuration
          ===============================================
Bridge:                  Enabled                 Bridge Behavior: STB
+---------+-----------| SOURCE ROUTING INFORMATION |-----------+---------+
Bridge Number:           N/A                     Segments:          0
Max ARE Hop Cnt:         00                      Max STE Hop cnt:   00
1 : N SRB:               Not Active              Internal Segment:  0x000
LF-bit interpret:        Extended
+---------+---------------| SR-TB INFORMATION |---------------+---------+
SR-TB Conversion:        Disabled
TB-Virtual Segment:      0x000                   MTU of TB-Domain:  0
+---------+-------| SPANNING TREE PROTOCOL INFORMATION |----------+------+
Bridge Address:          Default               Bridge Priority:   32768/0x8000
STP Participation:       IEEE802.1d
+---------+-----------| TRANSLATION INFORMATION |-------------+---------+
FA<=>GA Conversion:      Enabled                 UB-Encapsulation:  Disabled
DLS for the bridge:      Enabled
+---------+--------------| PORT INFORMATION |---------------+---------+
Number of ports added: 4
Port: 1      Interface: 0      Behavior: No Bridging   STP:  Enabled
Port: 2      Interface: 1      Behavior: No Bridging   STP:  Enabled
Port: 3      Interface: 2      Behavior: No Bridging   STP:  Enabled
Port: 4      Interface: 3      Behavior:    STB Only   STP:  Enabled
```

Figure 72. Configuring ASRT on the Data Center Router

Now we configure DLSw. This involves enabling it at the box level and also opening SAPs for the traffic that you want to carry across the DLSw connection. These steps are illustrated in Figure 73.

```
Li Config>p dls
DLSw protocol user configuration
Li DLSw config>enable dls
Data Link Switching is now enabled
Li DLSw config>set srb aaa
DLSw segment number has been set.
Li DLSw config>open-sap
Enter Interface number [0]? 3
Enter SAP in hex (range 0-FE), 'SNA', 'NB' or 'LNM'  [4]? sna
SAP(s)  0  4  8  C opened on interface 3
Li DLSw config>open-sap
Enter Interface number [0]? 3
Enter SAP in hex (range 0-FE), 'SNA', 'NB' or 'LNM'  [4]? nb
SAP(s) F0 opened on interface 3
Li DLSw config>list open
Interface SAP(s)
    3      0  4  8  C F0
```

Figure 73. Configuring DLSw on the Data Center Router

Now we add the DLSw neighbor (the other end of the DLSw pipe). The neighbor DLSw IP address added here must be the internal IP address of the peer DLSw router. In our case, this is the router at the other end of the IPSec tunnel although it could be any router in the branch office that has a valid IP connection.

In our example, the internal address has been set to the interface address of the public network (our IPSec tunnel endpoint). This has an implication regarding the configuration of the packet filters for IPSec. DLSw packets have source and destination IP addresses of the TCP connection endpoints which are the internal addresses of the two routers at the endpoints. Our packet filters need to have access controls that enable these DLSw packets to get through the tunnel.

```
Li DLSw config>add tcp
Enter the DLSw neighbor IP Address [0.0.0.0]? 192.168.189.59
Connectivity Setup Type (a/p) [p]? a
Transmit Buffer Size (Decimal) [5120]?
Receive Buffer Size (Decimal) [5120]?
Maximum Segment Size (Decimal) [1024]?
TCP Keepalive (E/D) [D]? e
NetBIOS SessionAlive Spoofing (E/D) [D]?
Neighbor Priority (H/M/L) [M]?
TCP Neighbor has been added
Li DLSw config>exit
Li Config>
Li *reload
Are you sure you want to reload the gateway? (Yes or [No]): yes
The configuration has been changed, save it? (Yes or [No] or Abort): yes
Config Save: Using bank A and config number 4
```

Figure 74. Configuring TCP Neighbors on the Data Center Router

This completes the configuration of the data center router. As shown in Figure 74, you need to restart or reload the router before the new DLSw configuration changes will become active.

4.1.2 Configuring the Branch Router

The configuration of the branch router will be the same as the data center router except that in the branch office, we have a token-ring segment instead of an Ethernet segment. So, we need to use source route bridging instead of transparent bridging.

The first step is to disable access control as shown in Figure 75.

```
Karen *t 6
Karen Config>p ip
Internet protocol user configuration

Karen IP config>set access-control off
Karen IP config>exit
Karen Config>
Karen *t 5
Karen +p ip
Karen IP>reset ip
Karen IP>exit
```

Figure 75. Temporarily Disabling Access Control on the Branch Router

The next step is to disable IPSec as shown in Figure 76 on page 58.

```
Karen *t 6
Karen Config>feature ip
IP Security feature user configuration
Karen IPsec config>disable ipsec stop
Karen IPsec config>exit
Karen Config>
Karen *
```

Figure 76. Temporarily Disabling IPSec on the Branch Router

The next step is to configure the bridging function as shown in Figure 77.

```
Karen Config>p asrt
Adaptive Source Routing Transparent Bridge user configuration
Karen ASRT config>ena bridge
Karen ASRT config>ena dls
```

Figure 77. Configuring ASRT on the Branch Router

Next, we list it back out to verify the changes as shown in Figure 78.

```
Karen ASRT config>list bridge

           Source Routing Transparent Bridge Configuration
           ===============================================
Bridge:                  Enabled                 Bridge Behavior: STB
+---------+-----------| SOURCE ROUTING INFORMATION |-----------+---------+
Bridge Number:           N/A                     Segments:          0
Max ARE Hop Cnt:         00                      Max STE Hop cnt:   00
1 : N SRB:               Not Active              Internal Segment:  0x000
LF-bit interpret:        Extended
+---------+---------------| SR-TB INFORMATION |---------------+---------+
SR-TB Conversion:        Disabled
TB-Virtual Segment:      0x000                   MTU of TB-Domain:  0
+---------+-------| SPANNING TREE PROTOCOL INFORMATION |----------+------+
Bridge Address:          Default               Bridge Priority:   32768/0x8000
STP Participation:       IEEE802.1d
+---------+-----------| TRANSLATION INFORMATION |-------------+---------+
FA<=>GA Conversion:      Enabled              UB-Encapsulation:  Disabled
DLS for the bridge:      Enabled
+---------+---------------| PORT INFORMATION |----------------+---------+
Number of ports added: 2
Port: 1      Interface: 0      Behavior:    STB Only   STP:  Enabled
Port: 2      Interface: 5      Behavior:    STB Only   STP:  Enabled
```

Figure 78. Configuring ASRT on the Branch Router

Next, we disable bridging in the interfaces not being used for this configuration. We then configure interface 5 (bridge port number 2) for Source Route Bridging (SRB) and give it a segment number. This is illustrated in Figure 79 on page 59.

```
Karen ASRT config>disa trans
Port Number [1]? 1
Karen ASRT config>disa trans
Port Number [1]? 2
Karen ASRT config>ena source
Port Number [1]? 2
Segment Number for the port in hex(1 - FFF) [001]? aa1
Bridge number in hex (0 - 9, A - F) [0]? 1
```

Figure 79. Configuring ASRT on the Branch Router

Now we configure DLSw. This is illustrated in Figure 80.

```
Karen Config>p dls
DLSw protocol user configuration
Karen DLSw config>ena dls
Data Link Switching is now enabled
Karen DLSw config>set srb aaa
DLSw segment number has been set.
Karen DLSw config>open-sap
Enter Interface number [0]? 5
Enter SAP in hex (range 0-FE), 'SNA', 'NB' or 'LNM'  [4]? sna
One or more SAPs already opened on interface 5
Karen DLSw config>open
Enter Interface number [0]? 5
Enter SAP in hex (range 0-FE), 'SNA', 'NB' or 'LNM'  [4]? nb
SAP F0 already opened on interface 5
Karen DLSw config>list open
Interface SAP(s)
    5      0  4  8  C F0
```

Figure 80. Configuring DLSw on the Branch Router

Add the DLSw neighbor (the other end of the pipe). This is the internal IP address of the 2210 in the branch. This is shown in Figure 81.

```
Karen DLSw config>add tcp
Enter the DLSw neighbor IP Address [0.0.0.0]? 192.168.189.1
Connectivity Setup Type (a/p) [p]? a
Transmit Buffer Size (Decimal) [5120]?
Receive Buffer Size (Decimal) [5120]?
Maximum Segment Size (Decimal) [1024]?
TCP Keepalive (E/D) [D]? e
NetBIOS SessionAlive Spoofing (E/D) [D]?
Neighbor Priority (H/M/L) [M]?
TCP Neighbor has been added
Karen *r
Are you sure you want to restart the gateway? (Yes or [No]): y
```

Figure 81. Configuring TCP Neighbors on the Branch Router

This completes the steps necessary for adding DLSw to our VPN configuration. As shown in Figure 81, you need to restart the router to make the DLSw changes active.

4.1.3 Testing DLSw

At this point, you would stop and test the DLSw configuration and make sure that it is working like you intended. You can see if the connection between the TCP neighbors is established and also if there is a DLS session. In Figure 82, you can see that a NetBIOS session has been established between PC B and PC A in our test network. This is indicated by the F0 Service Access Point (SAP) in the MAC address/SAP pairs for the DLS session.

```
Li *t 5
Li +p dls
Data Link Switching Console

Li DLSw>list tcp sess all
Group/Mcast@    IP Address      Conn State     CST Version  ActSes SesCreates
--------------- --------------- -------------- --- -------- ------ ----------
1               192.168.189.59  ESTABLISHED     a  AIW V2RO   1             1

Li DLSw>list dls sess all
    Source         Destination      State     Flags    Dest IP Addr    Id
---------------  ---------------  ---------  -------  --------------  ----
1 08005A5DB973 F0 400052005123 F0 CONNECTED           192.168.189.59    0

Li DLSw>exit
```

Figure 82. Testing DLSw

4.1.4 Re-enabling Access Control and IPSec

After we are satisfied that DLSw is working correctly, it is time to re-enable access control and IPSec.

Here we show how to do these steps for the router in the data center (the 2216 named Li). It is the same for the 2210 except that in the 2210, you use the restart command instead of the reload command as on the 2216. Figure 83 shows the command to re-enable access control.

```
Li *t 6
Li Config>p ip
Internet protocol user configuration
Li IP config>set access on
Li IP config>exit
Li Config>
```

Figure 83. Re-enabling Access Control

Figure 84 on page 61 shows the command to re-enable IPSec.

```
Li *t 6
Li Config>f ip
IP Security feature user configuration
Li IPsec config>enable ipsec
Restarting the router is required for IPsec to be active.
Li IPsec config>
```

Figure 84. Re-enabling IPSec

After enabling IPSec, you must restart the router in order to make the changes effective. When the router comes back up, IPSec and access control are enabled. Figure 85 shows the reload command for the router Li (2216).

```
Li *reload
Are you sure you want to reload the gateway? (Yes or [No]): yes
The configuration has been changed, save it? (Yes or [No] or Abort): yes
Config Save: Using bank A and config number 2
```

Figure 85. Reloading the 2216

4.1.5 Testing DLSw with IPSec Enabled

After restarting the router, we check to verify that IPSec and our tunnels are enabled. As shown in Figure 86 on page 62, you can use the `list all` command at the IPSec prompt.

From the figure, we can see that IPSec is enabled and both tunnels are enabled also. Tunnel number 2 is the important one for DLSw as that is the one that all our DLSw traffic will go through. Remember that tunnel 2 is a transport-mode tunnel and all packets that originate in the routers will go through this tunnel.

```
Li +f ip
Li IPsec>list all

IPsec is ENABLED

Defined Manual Tunnels:

   ID         Name         Local IP Addr   Remote IP Addr   Mode    State
 ------  ---------------  ---------------  ---------------  -----  ------
      1  ESP&AH             192.168.189.1   192.168.189.59  TUNN   Enable
      2  TRANS-ESP&AH       192.168.189.1   192.168.189.59  TRANS  Enable

Tunnel Cache:

 ID     Local IP Addr   Remote IP Addr   Mode   Policy  Tunnel Expiration
-----  ---------------  ---------------  -----  ------  -----------------
    2    192.168.189.1   192.168.189.59  TRANS  ESP-AH  10:21  Jun 20 199
    1    192.168.189.1   192.168.189.59  TUNN   ESP-AH  10:21  Jun 20 199
Li IPsec>exit
```

Figure 86. Testing DLSw with IPSec Enabled

Next, we verify that DLSw is still working with IPSec enabled. Figure 87 shows that the TCP and DLSw sessions are still active with IPSec enabled.

```
Li *t 5
Li +p dls
Data Link Switching Console

Li DLSw>list tcp sess all
Group/Mcast@    IP Address      Conn State     CST Version  ActSes SesCreates
--------------- --------------- -------------- --- -------- ------ ----------
1               192.168.189.59  ESTABLISHED     a  AIW V2RO   1             1

Li DLSw>list dls sess all
    Source         Destination      State     Flags    Dest IP Addr    Id
--------------  ---------------  ---------  -------  --------------  ----
1 08005A5DB973 F0 400052005123 F0 CONNECTED           192.168.189.59    0

Li DLSw>exit
```

Figure 87. Testing DLSw with IPSec Enabled

To make sure that the DLSw traffic is actually going through the IPSec tunnel, we check the IPSec statistics and see if the counters are increasing. Figure 88 on page 63 shows the statistics for tunnel number 2, the tunnel that handles the traffic originated by the routers that includes our DLSw traffic.

```
Li IPsec>stats
Enter the Tunnel ID, Tunnel Name, or 'ALL' [ALL]? 2

                          Global IPSec Statistics
Received:
  total pkts   AH packets   ESP packets   total bytes    AH bytes     ESP bytes
  ----------   ----------   -----------   -----------   ----------   ----------
      109788       109788        109788      22627872     12631392      9996480

Sent:
  total pkts   AH packets   ESP packets   total bytes    AH bytes     ESP bytes
  ----------   ----------   -----------   -----------   ----------   ----------
          30           30            30          5456         3328         2128

Receive Packet Errors:
  total errs    AH errors   AH bad seq   ESP errors   ESP bad seq
  ----------   ----------   ----------   ----------   -----------
           0            0            0            0             0

Send Packet Errors:
  total errs    AH errors   ESP errors
  ----------   ----------   ----------
           0            0            0

Li IPsec>
```

Figure 88. Checking the IPSec Statistics

Another way to check the number of packets that are going through the IPSec tunnel is to check the packet filter statistics and see how many times this filter was matched. Figure 89 on page 64 shows a listing of the outbound filter, but you can also check the inbound filter and see similar information.

In this case we are interested in access control numbers 3 and 4. The figure shows that these have been matched 597 times (Use=597). Remember that control number 4 is the control that funnels the DLSw traffic to the IPSec engine and control number 3 is the control that lets the IPSec packets out of the router after they have been through the IPSec code.

```
Li IP>pac pf_out_0
Name              Dir  Intf  State  Src-Addr-Ver  #Access-Controls
pf_out_0          Out  0     On     N/A           4

Access Control currently enabled
Access Control facility: USER

Access Control run 1208 times, 3570 cache hits

List of access control records:

1   Type=I S   Source=192.168.180.0    Dest=192.168.157.0    Prot=  0-255
               Mask=  255.255.255.0    Mask=255.255.255.0    Use=0
               SPorts=N/A              DPorts=N/A            Tid=1
                                       Log=No

2   Type=I S   Source=9.24.105.0       Dest=192.168.157.0    Prot=  0-255
               Mask=  255.255.255.0    Mask=255.255.255.0    Use=0
               SPorts=N/A              DPorts=N/A            Tid=1
                                       Log=No

3   Type=I     Source=192.168.189.1    Dest=192.168.189.59   Prot= 50-51
               Mask=  255.255.255.255  Mask=255.255.255.255  Use=597
               SPorts=    0-65535      DPorts=    0-65535
                                       Log=No

4   Type=I S   Source=192.168.189.1    Dest=192.168.189.59   Prot=  0-255
               Mask=  255.255.255.255  Mask=255.255.255.255  Use=597
               SPorts=N/A              DPorts=N/A            Tid=2
                                       Log=No
Li IP>
```

Figure 89. Checking the Packet Filters

Chapter 5. IP Bridging through an IPSec Tunnel

Another way to enable multiple protocols through our IPSec tunnel is to use the Bridging Tunnel feature of the IBM Nways 2210/2216 routers. The bridging tunnel (encapsulation) is another feature of the ASRT bridge software. By encapsulating packets in industry-standard TCP/IP packets, the bridging router can dynamically route these packets through large IP internetworks to the destination end stations.

End stations see the IP path (the tunnel) as a single hop, regardless of the network complexity. This helps overcome the usual 7-hop distance limit encountered in source routing configurations. It also lets you connect source-routing end stations across non-source-routing media like Ethernet networks.

Since the IP bridging tunnel uses IP packets, we can secure them using IPSec. This chapter shows you how to configure IP bridging over our VPN by using our IPSec tunnel defined in Chapter 3, “Connecting the Data Center to the Branch Office” on page 33.

5.1 Configuring IP Bridge Tunnel in an IPSec Environment

Figure 90 shows our sample network again with some additional MAC addresses that we use in this scenario.

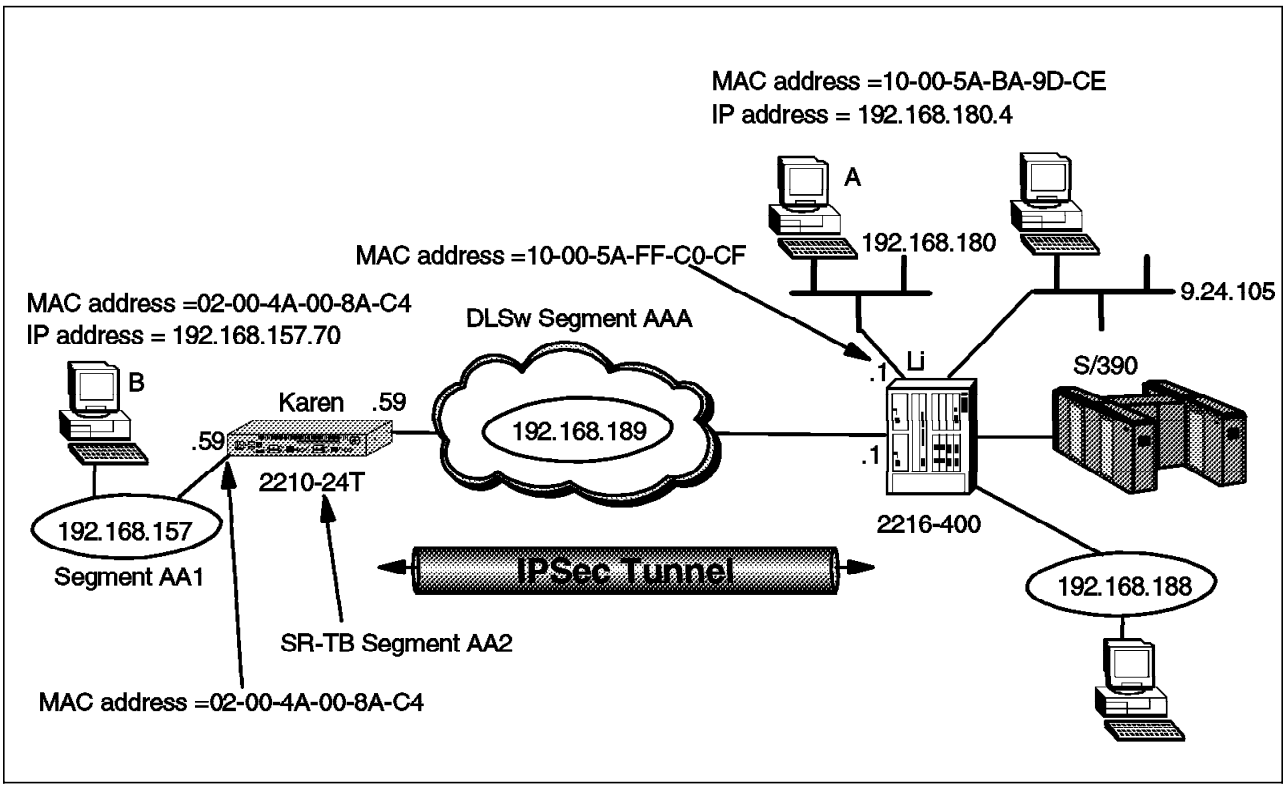


Figure 90. IP Bridging Tunnel through an IPSec Tunnel

For this scenario, we want the 2210 to be configured as a source route-translational bridge (SR-TB) with source route bridging (SRB) on token-ring

interface 5 (secure network side) and transparent bridging (STB) via IP tunnel on token-ring 0 (non-secure network).

We want the 2210 token-ring interface 0 to route IP. It has an IP address of 192.168.189.59 with a subnet mask of 255.255.255.0.

We want the 2216 to be a pure transparent bridge (STB) with STB enabled on the Ethernet interface and the token-ring interface 0 via our IP bridged tunnel.

We also want the 2216 token-ring interface 0 to route IP. It has an IP address of 192.168.189.1 with a subnet mask of 255.255.255.0.

We have an IPSec tunnel configured between the addresses 192.168.189.1 and 192.168.189.59 and we only allow packets from or to those addresses to go through the tunnel.

We have a PC configured with NetBIOS in the data center which is labeled PC A. Another PC, labeled PC B, is located in the branch office and is also configured with NetBIOS. From PC A we access a remote disk on PC B using the IP bridging tunnel which is passed through the IPSec tunnel.

As discussed in Chapter 4, “Data Link Switching over IPSec” on page 53, we recommend that you make these configuration additions and test them first with the IP packet filters and IPSec feature disabled. This will help you with problem determination if you experience any problems in setting up the bridged tunnel.

5.1.1 Configuring the 2210 Branch Router

The first step is to enable the Adaptive Source Route Transparent (ASRT) bridge function of the router. This command is shown in Figure 91 on page 67 along with the command to list the ASRT bridge characteristics.

Note: Listing the bridge configuration is an easy way to get the bridge port numbers that we need to set the port characteristics.

As can be seen from the figure, the ASRT bridge behavior defaults to transparent bridging (STB) while source route translational bridging (SR-TB) is disabled. Token-ring interface 0 is bridge port 1 while token-ring interface 5 is bridge port 2.

```
Karen config>p asrt
Adaptive Source Routing Transparent Bridge user configuration
Karen ASRT config>enable bridge
Karen ASRT config>list bridge

               Source Routing Transparent Bridge Configuration
               ===============================================
Bridge:                  Enabled                Bridge Behavior: STB
+----------+------------| SOURCE ROUTING INFORMATION |------------+----------+
Bridge Number:           N/A                    Segments:          0
Max ARE Hop Cnt:         00                     Max STE Hop cnt:   00
1 : N SRB:               Not Active             Internal Segment:  0x000
LF-bit interpret:        Extended
+----------+---------------| SR-TB INFORMATION |-----------------+----------+
SR-TB Conversion:        Disabled
TB-Virtual Segment:      0x000                  MTU of TB-Domain:  0
+----------+-------| SPANNING TREE PROTOCOL INFORMATION |---------+----------+
Bridge Address :         Default                Bridge Priority: 32768/0x8000
STP Participation :      IEEE802.1d
+----------+-------------| TRANSLATION INFORMATION |--------------+----------+
FA<=>GA Conversion:      Enabled             UB-Encapsulation:  Disabled
DLS for the bridge:      Disabled
+----------+-----------------| PORT INFORMATION |-----------------+----------+
Number of ports added: 2
Port:   1      Interface:    0      Behavior:    STB Only   STP:  Enabled
Port:   2      Interface:    5      Behavior:    STB Only   STP:  Enabled
```

Figure 91. Enabling the Bridge

Next, we need to disable the STB function since we do not use it on either of the token-ring ports (ports 1 and 2). We then enable SRB on port 2 and define the segment number attaching to this token-ring port to be AA1 and the 2210 bridge number to be 1. This is shown in Figure 92.

```
Karen ASRT config>disa transparent 1
Karen ASRT config>disa transparent 2
Karen ASRT config>enable source 2 AA1
Bridge number in hex (0 - 9, A - F) [0]? 1
```

Figure 92. Configuring Bridge Ports

As we have STB and SRB, we need to use Source Route-Translational Bridge (SR-TB) to translate a source route bridge frame into a transparent bridge frame and vice versa. SR-TB is enabled at the box level which is illustrated in Figure 93. The transparent bridge domain is seen as LAN segment number AA2 from the source route bridge domain.

```
Karen ASRT config>ena sr-tb
TB-Domain Segment Number in hex(1 - FFF) [1]? aa2
TB-Domain's MTU 1470?
Bridge Virtual Segment Number in hex(1 - FFF) [1]?
```

Figure 93. Configuring Translational Bridging

At this point, we define the IP bridging tunnel. This is done simply with the add tunnel command as shown in Figure 94 on page 68. As a result, a new bridge port is added with a default behavior of transparent bridging (STB).

```
Karen ASRT config>add tunnel
Port Number [3]? 3

                Source Routing Transparent Bridge Configuration
                ===============================================
Bridge:                  Enabled                 Bridge Behavior: STB
+----------+------------| SOURCE ROUTING INFORMATION |------------+----------+
Bridge Number:           N/A                     Segments:          0
Max ARE Hop Cnt:         00                      Max STE Hop cnt:   00
1 : N SRB:              Not Active             Internal Segment:  0x000
LF-bit interpret:        Extended
+----------+----------------| SR-TB INFORMATION |-----------------+----------+
SR-TB Conversion:        Disabled
TB-Virtual Segment:      0x000                   MTU of TB-Domain:  0
+----------+-------| SPANNING TREE PROTOCOL INFORMATION |---------+----------+
Bridge Address:          Default                 Bridge Priority:  32768/0x8000
STP Participation:       IEEE802.1d
+----------+-------------| TRANSLATION INFORMATION |--------------+----------+
FA<=>GA Conversion:      Enabled             UB-Encapsulation:  Disabled
DLS for the bridge:      Disabled
+----------+-----------------| PORT INFORMATION |-----------------+----------+

Number of ports added: 2
Port: 1    Interface:      0      Behavior: No Bridging   STP:  Enabled
Port: 2    Interface:      5      Behavior:    SRB Only   STP:  Enabled
Port: 3    Interface: Tunnel      Behavior:    STB Only   STP:  Enabled
```

Figure 94. Adding a Bridging Tunnel

We also need to specify the destination IP address of the other end of the IP bridging tunnel. This is shown in Figure 95 on page 69. The IP address of the other end of the IP bridging tunnel is the interface address and also the internal IP address of the router.

Note: It is very important to add the necessary access controls to the inbound and outbound packet filters for this router-to-router traffic so that the packets can be processed by IPSec. This was performed in 3.1.1, “Configuring the Branch Office Router” on page 34 and 3.1.1.1, “Defining the Inbound Packet Filters” on page 38 for the 2210.

```
Karen ASRT config>tunnel
Tunnel interface configuration

Karen TNL config>add address
Enter the address to be added [0.0.0.0]? 192.168.189.1
Karen TNL config>list all
IP Tunnel Addresses

     192.168.189.1

Karen TNL config>exit
Karen ASRT config>exit
```

Figure 95. Configuring a Bridging Tunnel

Finally, we restart the router to activate this configuration. This is illustrated in Figure 96.

```
Karen config>
*restart
Are you sure you want to restart the gateway? (Yes or [No]): Yes
```

Figure 96. Restarting the Router

5.1.2 Configuring the Data Center Router

We need to do the same steps almost exactly to configure the 2216 in the data center for our bridging tunnel. This section takes you step-by-step through this process.

Again, the first step is to enable the bridge and list the configuration so that we can see the port numbers that have been defined. This is illustrated in Figure 97 on page 70.

```
Li *t 6
Gateway user configuration
Li config>p asrt
Adaptive Source Routing Transparent Bridge user configuration
Li ASRT config>ena bridge
Li ASRT config>list bridge

                Source Routing Transparent Bridge Configuration
                ===============================================



Bridge:                  Enabled                  Bridge Behavior: STB
+----------+------------| SOURCE ROUTING INFORMATION |------------+----------+
Bridge Number:           N/A                      Segments:          0
Max ARE Hop Cnt:         00                       Max STE Hop cnt:   00
1 : N SRB:              Not Active               Internal Segment:  0x000
LF-bit interpret:        Extended
+----------+----------------| SR-TB INFORMATION |-----------------+----------+
SR-TB Conversion:        Disabled
TB-Virtual Segment:      0x000                    MTU of TB-Domain:  0
+----------+-------| SPANNING TREE PROTOCOL INFORMATION |---------+----------+
Bridge Address:          Default                  Bridge Priority: 32768/0x8000
STP Participation:       IEEE802.1d
+----------+-------------| TRANSLATION INFORMATION |--------------+----------+
FA<=>GA Conversion:      Enabled                  UB-Encapsulation:  Disabled
DLS for the bridge:      Disabled
+----------+-----------------| PORT INFORMATION |-----------------+----------+

Number of ports added: 4
Port: 1    Interface:       0      Behavior:    STB Only   STP:  Enabled
Port: 2    Interface:       1      Behavior:    STB Only   STP:  Enabled
Port: 3    Interface:       2      Behavior:    STB Only   STP:  Enabled
Port: 4    Interface:       3      Behavior:    STB Only   STP:  Enabled
```

Figure 97. Enabling the Bridge

Again, we disable the default STB behavior (in this example on all the interfaces except port 4 which is our Ethernet segment where we use transparent bridging). This is illustrated in Figure 98.

```
Li ASRT config>disa trans 1
Li ASRT config>disa trans 2
Li ASRT config>disa trans 3
```

Figure 98. Configuring Bridge Ports

Next, we add the IP bridging tunnel port. This is illustrated in Figure 99 on page 71. Note that the tunnel port is STB by default.

```
Li ASRT config>add tunnel
Port Number [5]? 5
Li ASRT config>list bridge

               Source Routing Transparent Bridge Configuration
               ===============================================

Bridge:                 Enabled                 Bridge Behavior: STB
+----------+------------| SOURCE ROUTING INFORMATION |------------+----------+
Bridge Number:          N/A                     Segments:          0
Max ARE Hop Cnt:        00                      Max STE Hop cnt:   00
1 : N SRB:             Not Active              Internal Segment:  0x000
LF-bit interpret:       Extended
+----------+---------------| SR-TB INFORMATION |-----------------+----------+
SR-TB Conversion:       Disabled
TB-Virtual Segment:     0x000                   MTU of TB-Domain:  0
+----------+-------| SPANNING TREE PROTOCOL INFORMATION |---------+----------+
Bridge Address:         Default                 Bridge Priority: 32768/0x8000
STP Participation:      IEEE802.1d
+----------+-------------| TRANSLATION INFORMATION |--------------+----------+
FA<=>GA Conversion:     Enabled                 UB-Encapsulation:  Disabled
DLS for the bridge:     Disabled
+----------+-----------------| PORT INFORMATION |-----------------+----------+

Number of ports added: 5
Port: 1    Interface:       0      Behavior: No Bridging   STP:  Enabled
Port: 2    Interface:       1      Behavior: No Bridging   STP:  Enabled
Port: 3    Interface:       2      Behavior: No Bridging   STP:  Enabled
Port: 4    Interface:       3      Behavior:    STB Only   STP:  Enabled
Port: 5    Interface:  Tunnel      Behavior:    STB Only   STP:  Enabled
```

Figure 99. Adding a Bridge Tunnel Port

Next, we add the destination IP address of the other side of the tunnel. This is illustrated in Figure 100.

```
Li ASRT config>tunnel
Tunnel interface configuration

Li TNL config>add address 192.168.189.59
Li TNL config>list all
IP Tunnel Addresses

     192.168.189.59

Li TNL config>exit
Li ASRT config>exit
Li config>
```

Figure 100. Configuring a Bridging Tunnel

Finally, we reload the router to activate the configuration. This is illustrated in Figure 101 on page 72.

```
Li *reload
Are you sure you want to reload the gateway? (Yes or [No]): yes
The configuration has been changed, save it? (Yes or [No] or Abort): yes
Config Save: Using bank A and config number 2
```

Figure 101. Reloading the Router

5.1.3 Testing the IP Bridging Tunnel (IPSec Disabled)

Now, we test the IP bridging tunnel configuration to make sure that it is working like we intended. After sending some NetBIOS traffic between PC A and PC B, we issue the `list database` command from talk 5 to see if our MAC addresses are dynamically registered to use the IP bridging tunnel. From the listing in Figure 102 on page 73, you can see:

- **Address 00-20-35-45-D3-95 :** This is the address for interface 5 of the router Karen, *the 2210 in the branch office*. This physical MAC address is dynamically registered *through the IP tunnel*.
- **Address 02-00-4A-00-8A-C4 :** This is the address for PC B that is attached to the SRB segment. As you can see, it is also dynamically registered.
- **Address 10-00-5A-BA-9D-CE :** This is the address for PC A that is connected to the STB segment. Here you see that this address is also dynamically registered on the Ethernet interface.
- **Address 10-00-5A-FF-C0-CF :** This is the address for the local Ethernet interface (bridge port 4) on the 2216. It does not use the IP bridge tunnel itself because it is a local interface.

```
Li ASRT>list database all
MAC Address    MC*  Entry Type       Age  Port(s)

00-20-35-45-D3-95   Dynamic           300  5 (IP Tunnel) @192.168.189.59
01-80-C2-00-00-00*  Registered             4-5
01-80-C2-00-00-01*  Reserved               All
01-80-C2-00-00-02*  Reserved               All
01-80-C2-00-00-03*  Reserved               All
01-80-C2-00-00-04*  Reserved               All
01-80-C2-00-00-05*  Reserved               All
01-80-C2-00-00-06*  Reserved               All
01-80-C2-00-00-07*  Reserved               All
01-80-C2-00-00-08*  Reserved               All
01-80-C2-00-00-09*  Reserved               All
01-80-C2-00-00-0A*  Reserved               All
01-80-C2-00-00-0B*  Reserved               All
01-80-C2-00-00-0C*  Reserved               All
01-80-C2-00-00-0D*  Reserved               All
01-80-C2-00-00-0E*  Reserved               All
01-80-C2-00-00-0F*  Reserved               All
02-00-4A-00-8A-C4   Dynamic           295  5 (IP Tunnel) @192.168.189.59
03-00-00-00-80-00*  Reserved               All
03-00-00-20-00-00*  Registered             1-2
10-00-5A-BA-9D-CE   Dynamic           295  4 (Eth /1         )
10-00-5A-FF-C0-CF   Registered             4 (Eth /1         )
```

Figure 102. Testing the IP Bridging Tunnel

5.1.4 Testing the IP Bridging Tunnel with IPSec Enabled

Now we re-enable access control, reset IP, then re-enable IPSec and reset the IPSec feature.

Next, we check the IPSec status as shown in Figure 103 on page 74 to make sure that IPSec has been re-enabled.

```
Li +f ip
Li IPsec>list all

IPsec is ENABLED

Defined Manual Tunnels:

   ID         Name         Local IP Addr   Remote IP Addr   Mode    State
 ------  ---------------  ---------------  ---------------  -----  ------
      1  ESP&AH             192.168.189.1   192.168.189.59  TUNN   Enable
      2  TRANS-ESP&AH       192.168.189.1   192.168.189.59  TRANS  Enable

Tunnel Cache:

 ID     Local IP Addr   Remote IP Addr   Mode   Policy  Tunnel Expiration
-----  ---------------  ---------------  -----  ------  -----------------
    2    192.168.189.1   192.168.189.59  TRANS  ESP-AH  15:32  Jun 21 199
    1    192.168.189.1   192.168.189.59  TUNN   ESP-AH  15:32  Jun 21 199
Li IPsec>exit
```

Figure 103. IPSec Status

Next, we check the IP bridging tunnel again to make sure that the tunnel is still working with IPSec enabled. As can be seen in Figure 104, the MAC addresses are still registered.

```
Li ASRT>list database all

MAC Address    MC*  Entry Type       Age  Port(s)

00-20-35-45-D3-95   Dynamic          250  5 (IP Tunnel) @192.168.189.59
01-80-C2-00-00-00*  Registered            4-5
01-80-C2-00-00-01*  Reserved              All
01-80-C2-00-00-02*  Reserved              All
01-80-C2-00-00-03*  Reserved              All
01-80-C2-00-00-04*  Reserved              All
01-80-C2-00-00-05*  Reserved              All
01-80-C2-00-00-06*  Reserved              All
01-80-C2-00-00-07*  Reserved              All
01-80-C2-00-00-08*  Reserved              All
01-80-C2-00-00-09*  Reserved              All
01-80-C2-00-00-0A*  Reserved              All
01-80-C2-00-00-0B*  Reserved              All
01-80-C2-00-00-0C*  Reserved              All
01-80-C2-00-00-0D*  Reserved              All
01-80-C2-00-00-0E*  Reserved              All
01-80-C2-00-00-0F*  Reserved              All
02-00-4A-00-8A-C4   Dynamic          245  5 (IP Tunnel) @192.168.189.59
03-00-00-00-80-00*  Reserved              All
03-00-00-20-00-00*  Registered            1-2
10-00-5A-BA-9D-CE   Dynamic          245  4 (Eth /1         )
10-00-5A-FF-C0-CF   Registered            4 (Eth /1         )
```

Figure 104. Testing IP Bridging with IPSec Enabled

Finally, in order to be sure that the IP bridging traffic is going through the IPSec tunnel, we list the IPSec statistics and check to see that the counters are

increasing. This is shown in Figure 105 on page 75. Note that tunnel number 2 is the one that we defined to carry the router-to-router traffic. As we send more traffic through the IP bridging tunnel, the counters for IPSec tunnel number 2 increase.

```
Li IPsec>stats
Enter the Tunnel ID, Tunnel Name, or 'ALL' [ALL]? 2

                          Global IPSec Statistics
Received:
  total pkts   AH packets   ESP packets   total bytes    AH bytes     ESP bytes
  ----------   ----------   -----------   -----------   ----------   ----------
        5792         5792          5792       1193952       666480       527472

Sent:
  total pkts   AH packets   ESP packets   total bytes    AH bytes     ESP bytes
  ----------   ----------   -----------   -----------   ----------   ----------
         478          478           478         88592        53856        34736

Receive Packet Errors:
  total errs    AH errors   AH bad seq   ESP errors   ESP bad seq
  ----------   ----------   ----------   ----------   -----------
           0            0            0            0             0

Send Packet Errors:
  total errs    AH errors   ESP errors
  ----------   ----------   ----------
           0            0            0

Li IPsec>
```

Figure 105. Checking the IPSec Statistics

Next, we check the number of times that the access controls on our IP packet filter have been matched. You can see in Figure 106 on page 76 that access control number 4 has been matched 434 times (use=434). This is the IPSec control for the router-to-router traffic (including our IP bridging traffic). Our traffic is first *caught* by this control and passed to IPSec for encapsulation after which it is sent through the filters again. The second time through the filters, access control number 3 is matched. This is because the traffic now has a protocol field that indicates that it is IPSec traffic (Protocol=50-51). Access control number 3 is an inclusive control that tells the router to let these packets out of the interface.

```
Li IP>pac pf_out_0
Name              Dir  Intf  State  Src-Addr-Ver  #Access-Controls
pf_out_0          Out  0     On     N/A           4

Access Control currently enabled
Access Control facility: USER

Access Control run 893 times, 8770 cache hits

List of access control records:

1   Type=I S   Source=192.168.180.0    Dest=192.168.157.0    Prot=  0-255
               Mask=  255.255.255.0    Mask=255.255.255.0    Use=0
               SPorts=N/A              DPorts=N/A            Tid=1
                                       Log=No

2   Type=I S   Source=9.24.105.0       Dest=192.168.157.0    Prot=  0-255
               Mask=  255.255.255.0    Mask=255.255.255.0    Use=0
               SPorts=N/A              DPorts=N/A            Tid=1
                                       Log=No

3   Type=I     Source=192.168.189.1    Dest=192.168.189.59   Prot= 50-51
               Mask=  255.255.255.255  Mask=255.255.255.255  Use=434
               SPorts=    0-65535      DPorts=    0-65535
                                       Log=No

4   Type=I S   Source=192.168.189.1    Dest=192.168.189.59   Prot=  0-255
               Mask=  255.255.255.255  Mask=255.255.255.255  Use=434
               SPorts=N/A              DPorts=N/A            Tid=2
                                       Log=No
Li IP>
```

Figure 106. Checking the Packet Filter Statistics

Chapter 6. APPN through an IPSec Tunnel

Advanced Peer-to-Peer Networking (APPN) is another very important protocol to transport across our virtual private network. Fortunately, the Enterprise Extender feature of MRS/MAS allows us to transport our APPN High Performance Routing (HPR) traffic over an IP backbone, in this case, the Internet. Since Enterprise Extender (also called HPR over IP) uses IP encapsulation, we can use IPSec to protect these packets as they traverse the public network.

In our scenario, (see Figure 107) we have an APPN end node (EN) in the branch office that needs to communicate with another EN in the data center. In the figure, these devices are labeled VPNOS2A and VPNWNTA, respectively. The 2210 router (named Karen) in the branch is configured as an APPN network node (NN) and is providing APPN directory services for device VPNOS2A. The 2216 (named Li) is also configured as a NN and is providing directory services for device VPNWNTA.

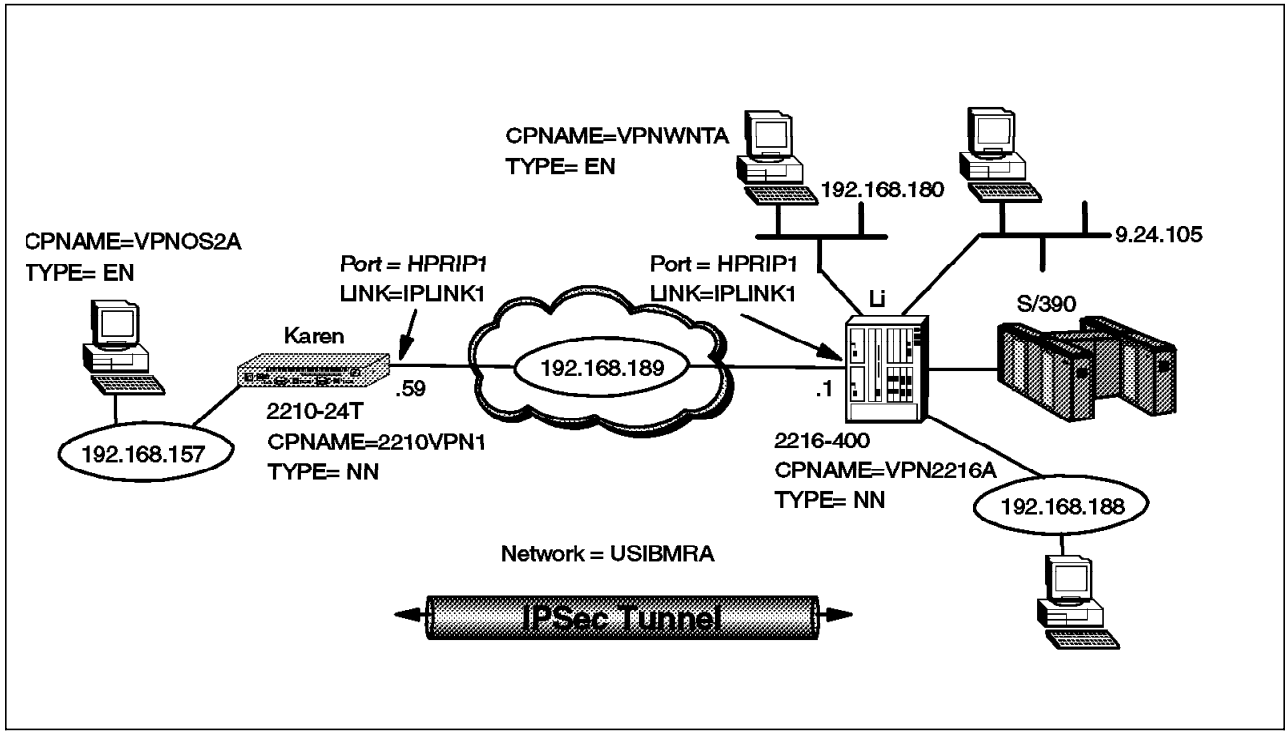


Figure 107. APPN through an IPSec Tunnel

The APPN traffic comes into the branch router as an LLC frame over the token-ring interface (which is also defined as an APPN port). The branch router, acting as an APPN network node, decides to route the traffic to its destination over the HPR over IP port. The HPR over IP engine in the router encapsulates the APPN LLC frame into an IP packet (using UDP) and then passes it to the IP routing element. IP then sends the packet to the other token-ring interface (our interface to the public network).

At this point, the outbound packet filter that we define on the token-ring interface redirects the packet to the IPSec engine where it is processed for AH and ESP headers before being sent out on the physical interface.

A similar process occurs in the reverse direction. As the IP packet reaches the end of the tunnel, it gets decapsulated and decrypted by the IPSec engine, then passed to the IP stack where it is determined that it must be directed to the HPR over IP port in the router. The HPR over IP function strips off the IP and UDP headers and passes the APPN LLC frame to APPN. The APPN network node routes the frame to its destination.

As discussed in 3.1.1, "Configuring the Branch Office Router" on page 34, we could use either an IPSec tunnel-mode tunnel or a transport-mode tunnel. One reason a company would use tunnel mode versus transport mode is to hide internal IP addresses used in the network.[1] When packets use tunnel mode, they are encapsulated with a new IP header and the original source and destination addresses are no longer visible.

However, in the case of HPR over IP packets, the IP traffic originates in the router where the APPN traffic is encapsulated and terminates in the router where it is decapsulated. In our scenario, the routers where the APPN traffic is encapsulated are the same routers used as our IPSec tunnel endpoints. In other words, only the Internet addresses of these two routers will appear in the HPR over IP packets. Using tunnel mode in this situation does not offer any advantages over transport mode in terms of hiding the source and destination IP addresses of the sender and receiver.

For our scenario, we chose to implement a transport-mode tunnel to carry our APPN traffic (as well as all the other router-to-router traffic). This tunnel was defined in Figure 54 on page 44.

6.1.1 Configuring the 2216 in the Data Center

Before we can configure APPN on the 2216, we first have to load the APPN package. This is shown in Figure 108. Once this command has been issued, the APPN module will be loaded during each subsequent IPL of the router.

Note: You must have an MAS software load that contains the APPN.LD file in order for this work.

```
Li *t 6

Li Config>load add package appn
appn package configured successfully
Li Config>
Li *reload
Are you sure you want to reload the gateway? (Yes or [No]): yes
The configuration has been changed, save it? (Yes or [No] or Abort): yes
Config Save: Using bank A and config number 3
The configuration has been saved.
```

Figure 108. Configuring the Necessary 2216 Code Elements

After the router comes back up, we go to the talk 6 APPN protocol menus and set the APPN node characteristics. This is done via the *set node* command as shown in Figure 109 on page 79.

[1] Another reason is to use unregistered IP addresses.

```
Li Config>protocol appn
Li APPN config>set node
Enable APPN (Y)es (N)o [Y]?
Network ID (Max 8 characters) [ ]? usibmra
Control point name (Max 8 characters) [ ]? vpn2216a
Enable branch extender or border node
        (0=Neither, 1=Branch Extender, 2=Border Node) [0]?
Route addition resistance(0-255) [128]?
XID ID number for subarea connection (5 hex digits) [00000]?
Use enhanced #BATCH COS (Y)es (N)o [Y]?
Use enhanced #BATCHSC COS (Y)es (N)o [Y]?
Use enhanced #INTER COS (Y)es (N)o [Y]?
Use enhanced #INTERSC COS (Y)es (N)o [Y]?
Write this record? [Y]?
The record has been written.
Li APPN config>
```

Figure 109. Defining the APPN Node on the 2216

As you can see, the only parameters that are absolutely necessary are the APPN CP name and the Network ID. The other parameters can be left at their default values.

The next step is to add the APPN ports that will be used to carry our APPN traffic. In Figure 110, we add an HPR over IP port.

```
Li APPN config>add port
APPN Port
Link Type: (P)PP, (FR)AME RELAY, (E)THERNET, (T)OKEN RING,
(M)PC, (S)DLC, (X)25, (FD)DI, (D)LSw, (A)TM, (I)P  [ ]? I
Port name (Max 8 characters) [IP65535]? HPRIP1
Enable APPN on this port (Y)es (N)o [Y]?
Port Definition
        Service any node: (Y)es (N)o [Y]?
        Maximum BTU size (768-2048) [1469]?
        UDP port number for XID exchange (1024-65535) [12000]?
        UDP port number for low priority traffic (1024-65535) [12004]?
        UDP port number for medium priority traffic (1024-65535) [12003]?
        UDP port number for high priority traffic (1024-65535) [12002]?
        UDP port number for network priority traffic (1024-65535) [12001]?
        IP Network Type: 0 = CAMPUS, 1 = WIDEAREA [0]?
        Enable IP Precedence: (Y)es (N)o [N]? Y
        Local SAP address (04-EC) [4]?
        LDLC Retry Count(1-255) [3]?
        LDLC Timer Period(1-255 seconds) [15]?
Would you like TG characteristics updated to recommended
values based on config changes: (Y)es (N)o [N]?
Edit TG Characteristics: (Y)es (N)o [N]?
Write this record? [Y]?
The record has been written.
Li APPN config>
```

Figure 110. Adding an APPN Port for HPR over IP

Again, we use the defaults for most of the parameters. The critical one is the port type (I for HPR over IP). Note that you don't need to specify an interface

number because there is only one HPR over IP port per router. We also give it a port name that we can easily recognize on the monitoring console.

Note: One new question on this screen in MAS/MRS V3.1 deals with the IPv4 precedence bits. If you respond yes to this question to enable setting of the precedence bits, then the 3 precedence bits in the TOS field of the IPv4 header will be set based on the HPR priority of the traffic. This allows you to preserve your SNA priorities using the Bandwidth Reservation System (BRS) feature even on encrypted packets. Please see *Nways Multiprotocol Access Services Protocol Configuration and Monitoring Reference, Volume 2*, SC30-3885 for more information.

Next, we add a link station on the newly-defined HPR over IP port. This is shown in Figure 111.

```
Li APPN config>add link
APPN Station
Port name for the link station [ ]? HPRIP1
Station name (Max 8 characters) [ ]? IPLINK1
        Activate link automatically (Y)es (N)o [Y]?
        IP address of adjacent node  [192.168.189.59]?
        Adjacent node type: 0 = APPN network node,
        1 = APPN end node or Unknown node type  [0]?
        Allow CP-CP sessions on this link (Y)es (N)o [Y]?
        CP-CP session level security (Y)es (N)o [N]?
        Configure CP name of adjacent node: (Y)es (N)o [N]?
        Remote SAP(04-EC) [4]?
        IP Network Type: 0 = CAMPUS, 1 = WIDEAREA [0]?
        LDLC Retry Count(1-255) [3]?
        LDLC Timer Period(1-255 seconds) [15]?
Would you like TG characteristics updated to recommended
values based on config changes: (Y)es (N)o [N]?
Edit TG Characteristics: (Y)es (N)o [N]?
Write this record? [Y]?
The record has been written.
Li APPN config>
```

Figure 111. Adding a Link Station for the HPR over IP Link

By specifying the port name for this link station, the router knows that it is an HPR over IP port. Therefore, it knows to prompt you for an IP address as opposed to a MAC address that it would need if we were defining a link station for a LAN port.

The IP address that we specify is the *internal address* of the 2210 in the branch office. This is the endpoint of our HPR over IP network. The other end of the HPR over IP link is always at the router that will decapsulate the packets and *not* the next hop router in the path. Intermediate routers, if any, merely perform IP routing on the encapsulated packets.

Note: The router internal address is configured from the talk 6 `protocol ip` prompt.

Next we add a port on the Ethernet LAN interface 3 so that stations on that LAN can set up link stations to the 2216. This is shown in Figure 112 on page 81.

```
Li APPN config>add port
APPN Port
Link Type: (P)PP, (FR)AME RELAY, (E)THERNET, (T)OKEN RING,
(M)PC, (S)DLC, (X)25, (FD)DI, (D)LSw, (A)TM, (I)P  [ ]? e
Interface number(Default 0): [0]? 3
Port name (Max 8 characters) [E00003]? TOWNTA
Enable APPN on this port (Y)es (N)o [Y]?
Port Definition
        Support multiple PU (Y)es (N)o [N]?
        Service any node: (Y)es (N)o [Y]?
        High performance routing: (Y)es (N)o [Y]?
        Maximum BTU size (768-1496) [1289]?
        Maximum number of link stations (1-976) [512]?
        Percent of link stations reserved for incoming calls (0-100) [0]?
        Percent of link stations reserved for outgoing calls (0-100) [0]?
        Local SAP address (04-EC) [4]?
        Local HPR SAP address (04-EC) [C8]?
Edit TG Characteristics: (Y)es (N)o [N]?
Edit LLC Characteristics: (Y)es (N)o [N]?
Edit HPR defaults: (Y)es (N)o [N]?
Write this record? [Y]?
The record has been written.
Li APPN config>
```

Figure 112. Adding the APPN Port for the 2216 Ethernet Interface

We do not need to define any link stations on this port as the workstations (APPN end nodes) will create implicit links when they initialize with their network node (in this case, the 2216 itself).

This completes the configuration of the 2216 in the data center. To activate the changes, we reload the router as shown in Figure 113.

```
Li Config>
Li *reload
Are you sure you want to reload the gateway? (Yes or [No]): yes
The configuration has been changed, save it? (Yes or [No] or Abort): yes
Config Save: Using bank A and config number 3
The configuration has been saved.
```

Figure 113. Reloading the 2216 in the Data Center

6.1.2 Configuring the 2210 in the Branch Office

This section takes you step-by-step through the APPN configuration of the 2210 in the branch office. (Please refer back to Figure 107 on page 77 to see the network diagram.) The steps are almost identical to the ones for configuring the 2216 in the data center.

First we set the APPN node characteristics. This is shown in Figure 114 on page 82.

```
Karen Config>p appn
Karen APPN config>set node
Enable APPN (Y)es (N)o [Y]?
Network ID (Max 8 characters) [  ]? usibmra
Control point name (Max 8 characters) [  ]? vpn2210a
Enable branch extender or border node
        (0=Neither, 1=Branch Extender, 2=Border Node) [0]?
Route addition resistance(0-255) [128]?
XID ID number for subarea connection (5 hex digits) [00000]?
Use enhanced #BATCH COS (Y)es (N)o [Y]?
Use enhanced #BATCHSC COS (Y)es (N)o [Y]?
Use enhanced #INTER COS (Y)es (N)o [Y]?
Use enhanced #INTERSC COS (Y)es (N)o [Y]?
Write this record? [Y]?
The record has been written.
Karen APPN config>
```

Figure 114. Setting the APPN Node Characteristics for the Branch Router

Note: The network ID must match at both ends of the HPR over IP link.

Next, we add an HPR over IP port. This is shown in Figure 115.

```
Karen APPN config>add port
APPN Port
Link Type: (P)PP, (FR)AME RELAY, (E)THERNET, (T)OKEN RING,
(S)DLC, (X)25, (FD)DI, (D)LSw, (A)TM, (I)P  [ ]? I
Port name (Max 8 characters) [IP65535]? HPRIP1
Enable APPN on this port (Y)es (N)o [Y]?
Port Definition
        Service any node: (Y)es (N)o [Y]?
        Maximum BTU size (768-2048) [1469]?
        UDP port number for XID exchange (1024-65535) [12000]?
        UDP port number for low priority traffic (1024-65535) [12004]?
        UDP port number for medium priority traffic (1024-65535) [12003]?
        UDP port number for high priority traffic (1024-65535) [12002]?
        UDP port number for network priority traffic (1024-65535) [12001]?
        IP Network Type: 0 = CAMPUS, 1 = WIDEAREA [0]? 1
        Enable IP Precedence: (Y)es (N)o [N]? Y
        Local SAP address (04-EC) [4]?
        LDLC Retry Count(1-255) [3]?
        LDLC Timer Period(1-255 seconds) [15]?
Would you like TG characteristics updated to recommended
values based on config changes: (Y)es (N)o [N]?
Edit TG Characteristics: (Y)es (N)o [N]?
Write this record? [Y]?
Karen APPN config>
```

Figure 115. Adding the HPR over IP Port for the Branch Router

Note that we use the same port name as we used for the 2216. This is just for our convenience as the port name is only used at the router where it is defined and has no correlation to any other port names on any other routers.

Now that we have the port defined, the next step would normally be to define a link station to the next hop APPN node. However, in this case, it is not

necessary because an implicit link will be created when the 2216 in the data center establishes a connection with this router in the branch office.

Next, we add a token-ring APPN port for LAN connected end nodes to connect to the 2210 as their NN server. This is shown in Figure 116.

```
Karen APPN config>add port
APPN Port
Link Type: (P)PP, (FR)AME RELAY, (E)THERNET, (T)OKEN RING,
(S)DLC, (X)25, (FD)DI, (D)LSw, (A)TM, (I)P  [ ]? T
Interface number(Default 0): [0]? 5
Port name (Max 8 characters) [TOOOO5]? TOOS2CS
Enable APPN on this port (Y)es (N)o [Y]?
Port Definition
        Support multiple PU (Y)es (N)o [N]?
        Service any node: (Y)es (N)o [Y]?
        High performance routing: (Y)es (N)o [Y]?
        Maximum BTU size (768-17745) [2048]?
        Maximum number of link stations (1-976) [512]?
        Percent of link stations reserved for incoming calls (0-100) [0]?
        Percent of link stations reserved for outgoing calls (0-100) [0]?
        Local SAP address (04-EC) [4]?
        Local HPR SAP address (04-EC) [C8]?
Edit TG Characteristics: (Y)es (N)o [N]?
Edit LLC Characteristics: (Y)es (N)o [N]?
Edit HPR defaults: (Y)es (N)o [N]?
Write this record? [Y]?
The record has been written.
Karen APPN config>
```

Figure 116. Adding an APPN Port for the LAN Interface on the Branch Router

This completes the APPN definition on the branch router. We restart the gateway to activate APPN as shown in Figure 117.

```
Karen Config>
Karen *restart
Are you sure you want to restart the gateway? (Yes or [No]): yes
```

Figure 117. Restarting the Router

6.1.3 Testing the APPN Configuration

To test the APPN setup, we go to the talk 5 APPN GWCON on the branch router and list the active links. This is shown in Figure 118 on page 84.

```
Karen *t 5


CGW Operator Console

Karen +p appn
APPN GWCON
Karen APPN >list link
    Name   Port Name  Intf       Adj CP Name  Type       HPR      State
========================================================================
 IPLINK1      HPRIP1     7   USIBMRA.VPN2216A   NN    ACTIVE     ACT_LS
     @@0     TOOS2CS     5   USIBMRA.VPNOS2A    EN    ACTIVE     ACT_LS
```

Figure 118. Listing the Status of the APPN Links on the Branch Router

From the figure, one thing that you can see is that an end node (USIBMRA.VPNOS2A) is connected over the Token-Ring port (TOOS2CS) via an implicit link (@@0).

However, more important to our VPN discussion is that the HPR over IP link to the 2216 in the data center (USIBMRA.VPN2216A) is active. We know that this traffic is going over the IPSec tunnel because we are using the same IPSec configuration and IP filters that we used in all previous scenarios. This configuration stipulates that all router-to-router traffic will be sent via transport mode over IPSec tunnel number 2. (Please see Chapter 3, “Connecting the Data Center to the Branch Office” on page 33 for a description of the transport-mode tunnel definition.)

Note: If the HPR over IP link does not become active, first re-check your configuration. If the configuration looks correct, try and ping each router′s internal address: first from the router to its own internal address, then to the other router′s internal address. Repeat this test from the other router. The internal address of each router must be reachable in order for the HPR over IP link to function.

Chapter 7. Adding Dependent LU Requester

The dependent LU requester (DLUR) feature available in both MRS and MAS allows you to connect PU Type 2.0 or T2.1 devices containing dependent LUs to your SNA host via APPN. The DLUR function in the router works in conjunction with a dependent LU server (DLUS) located in VTAM. The router can either be configured as an APPN network node or an APPN end node.

In our VPN scenario (see Figure 119), we have some T2.0 devices (and their associated dependent LUs) in the branch that we want to connect back to the data center. We put the DLUR function in the branch router, then use APPN transport between the DLUR and VTAM. Then, we use HPR over IP to carry the APPN traffic over the IP backbone (the Internet in this case) and hence, IPSec to protect these packets.

Further, with the new support for setting the IP precedence bits that became available in MRS/MAS Version 3.1, you can map the SNA priority (for example, HPR) of these connections into the IP packets.

Note: This priority is preserved even if you are using IPSec tunnel mode, where the original packet is completely encapsulated in another one.

7.1 Configuring DLUR in an IPSec Environment

Figure 119 shows the configuration that we used in this scenario.

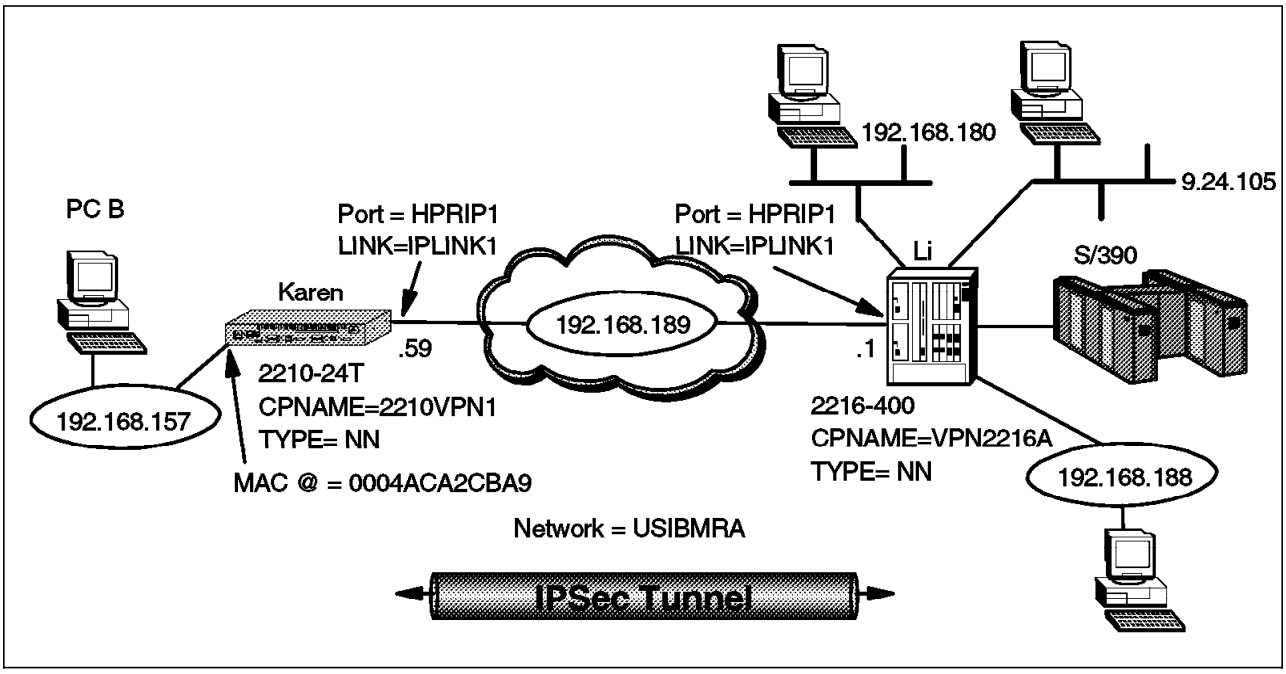


Figure 119. DLUR Using HPR over IP through an IPSec Tunnel

For our scenario, we use a PC with Personal Communications for OS/2 (PCOMM) as our PU T2.0 with a dependent LU. This machine is labeled PC B in the diagram. We configure PC B to access the host via the DLUR in the 2210 by simply providing the MAC address of the token-ring interface on the 2210 as the

LAN destination MAC address for the 3270 gateway. The MAC address of the 2210 interface is 0004ACA2CBA9.

As for the 2210 configuration, we use the same environment that we used in Chapter 6, “APPN through an IPSec Tunnel” on page 77, except that we enable DLUR support in the router.

In the 2216, we use an MPC+ connection over the ESCON channel to VTAM.[2] This is a very high performance connection and will generally provide the highest data throughout. Additionally, the required APPN support for DLUR is available over MPC+. Not shown in the figure is an IBM 9032 ESCON Director (ESCD) between the 2216 and the S/390.

To configure it, we simply define the MPC+ connection and then add an APPN port for this new connection to the existing APPN configuration that we used in Chapter 6, “APPN through an IPSec Tunnel” on page 77. Also as in that scenario, we use HPR over IP between the routers and send that traffic through the IPSec tunnel already configured between them.

7.1.1 VTAM Definitions

In this section, we present the basic VTAM definitions we used for our scenario. This is not meant to be a complete reference on the subject. For more information on configuring VTAM, refer to *CS OS/390 Resource Definition Reference*, SC31-8565.

DLUS support requires that VTAM be configured as an APPN network node. This requires certain parameters to be specified in the VTAM startup parameters to specify the use of APPN and HPR. These are shown in Figure 120 on page 87. Set the CONNTYPE to APPN and the NODETYPE to a Network Node (NN).

[2] Multi-Path Channel (MPC) is a protocol layer which allows multiple read and write subchannels to be treated as a single transmission group between the host and channel-attached devices. This interface is used by VTAM for APPN data transport. For more information about MPC+, refer to *IBM 2216 Multiaccess Connector ESCON Solutions*, SG24-2137.

```
ASYDE=TERM,IOPURGE=5M,
CONFIG=IO,
CONNTYPE=APPN,
CPCP=YES,
CSALIMIT=0,
DYNADJCP=YES,
ENCRYPTN=NO,
GWSSCP=YES,
HOSTPU=ISTPUS18,
HOSTSA=18,
HPR=RTP,
NETID=USIBMRA,
NODETYPE=NN,
NOTRACE,TYPE=VTAM,IOINT=0
PPOLOG=YES
SORDER=APPN,
SSCPDYN=YES,
SSCPID=18,
SSCPNAME=RAI,
SSCPORD=PRIORITY,
SUPP=NOSUP,
TNSTAT,CNSL,
VRTG=YES
OSITOPO=LLINES,
OSIMGMT=YES
XNETALS=YES
```

Figure 120. VTAM Startup Parameters

7.1.2 VTAM Definitions for an MPC+ Connection

An MPC+ connection requires entries in two VTAM control blocks:

- The Local major node
- The Transport Resource List (TRL) major node

Figure 121 shows a sample definition for a local SNA major node for a 2216 MPC+ connection. This is the local PU that resides in VTAM that supports the channel connection defined in the TRL. The connection type must be APPN and you also need to enable HPR.

```
LOCNETU VBUILD TYPE=LOCAL
LNETU   PU     TRLE=LNETU,
               XID=YES,
               CONNTYPE=APPN,
               CPCP=YES,
               HPR=YES
```

Figure 121. VTAM Local Major Node Definition

Notes:

1. TYPE must equal LOCAL on the VBUILD statement.
2. TRLE identifies the TRL being used. The name must match the name of an existing TRL.
3. XID indicates whether XIDs will be exchanged. It must be XID=YES.
4. CONNTYPE must be set to CONNTYPE=APPN since APPN is the only protocol that VTAM uses with an MPC+ connection.
5. CPCP specifies that CP-CP connections with APPN can be established over this MPC+ connection. This could be either set to YES or NO, depending upon your APPN topology.
6. HPR specifies that APPN HPR traffic can flow over this MPC+ connection. HPR is normally used by default, but setting this value to YES ensures it. This is important because an MPC+ connection requires RTP (and HPR).

Next, you need a transport resource list for the MPC+ connection from the 2216. An example definition is shown in Figure 122.

```
      VBUILD TYPE=TRL
LNETU TRLE   LNCTL=MPC,
             MAXBFRU=9,
             READ=280,
             WRITE=281,
             MPCLEVEL=HPDT,
             REPLYTO=3.0
```

Figure 122. VTAM Transport Resource List (TRL) Definition

Notes:

1. TYPE must be TRL.
2. LNETU is the name that identifies the TRL. It must match what is specified in the TRLE= field in the local major node definition. (See Figure 121 on page 87.)
3. LNCTL identifies the connection type. It must be LCNTL=MPC.
4. MAXBFRU is the number of 4K pages per read subchannel.
5. READ/WRITE specifies the subchannels in the MPC+ group, and indicates their direction. The subchannel numbers must be in the range of addresses specified in the IODEVICE statement in the IOCP definition. There can be multiple READ and WRITE parameters in the TRLE statement but there must be at least one of each.

   Note: The designations READ and WRITE here are from the HOST perspective. In the 2216 MPC+ definition, the designations are from the 2216 perspective. Therefore, subchannels designated as READ on the host **must** be designated as WRITE on the 2216, and vice versa.
6. REPLYTO is the reply timeout value in seconds.

7.1.3 Configuring the 2216 for MPC+

In this section, we show the steps necessary to:

1. Configure the 2216 for an ESCON MPC+ connection to the host
2. Add an APPN port for this connection

In order to connect the 2216 to the host using the ESCON adapter, you first need to add an ESCON interface for the router and configure it. Figure 123 shows this step. As can be seen from the figure, if you list the devices after adding the ESCON adapter, it will appear at the bottom of the list. You should check that the slot number is correct. Also remember that the interface numbers are dependent on the order in which you added the devices to the configuration.

```
Li *t 6
Gateway user configuration
Li Config>add device escon
Device Slot #(1-8) [1]? 3
Adding ESCON Channel device in slot 3  port 1 as interface #6
Use "net 6" to configure ESCON Channel parameters
Li Config>list dev
Ifc 0     Token Ring                        Slot: 1   Port: 1
Ifc 1     Token Ring                        Slot: 1   Port: 2
Ifc 2     Ethernet                          Slot: 5   Port: 1
Ifc 3     Ethernet                          Slot: 5   Port: 2
Ifc 4     V.35/V.36 PPP                     Slot: 6   Port: 0
Ifc 5     V.35/V.36 Frame Relay             Slot: 6   Port: 1
Ifc 6     ESCON Channel                     Slot: 3   Port: 1
```

Figure 123. Adding the ESCON Adapter

Now that we have the ESCON interface defined we need to add the MPC+ virtual interface. This MPC *virtual net handler* will perform all the MPC protocol functions for our connection to the host. Figure 124 shows this step.

```
Li Config>net 6
Li ESCON Config>add mpc
```

Figure 124. Adding the MPC+ Virtual Interface

As can be seen from Figure 125 on page 90, the prompt will change to the ESCON Add Virtual> prompt. From here you define the read and write subchannels that will be used for this connection.

```
Li ESCON Add Virtual>sub addr
Li ESCON Add MPC+ Read Subchannel>device
Device address (range 0x00-0xFF): [0]? 1
Li ESCON Add MPC+ Read Subchannel>link
Link address (ESCD Port) (range 0x01-0xFE): [1]? cc
Li ESCON Add MPC+ Read Subchannel>cu
Control Unit Logical Address (range 0x0-0xF): [0]? 0
Li ESCON Add MPC+ Read Subchannel>lpar
LPAR number (range 0x0-0xf): [0]? 1
Li ESCON Add MPC+ Read Subchannel>exit
```

Figure 125. Adding a Read Subchannel

You will need to provide the appropriate values for the following parameters:

Device address The unit address transmitted on the channel path to select the 2216 over another device on the channel. It is also referred to as subchannel number in S/370 I/O architecture. It is a two-digit hexadecimal value that may range from 00-FF. This value is defined in the host Input/Output Configuration Program (IOCP) by the UNITADD statement on the CNTLUNIT macro instruction for the real device. The value entered here will relate to the entry made in the TRL major node in VTAM for the *write* subchannel address. Remember that the write subchannel defined to VTAM will be your read subchannel for the 2216 and vice versa. (See Figure 126 on page 91.)

Link address The ESCON Director (ESCD) port number which is attached to the *host*. Note that this is *not* the ESCD port number on which the 2216 is attached. If you are using EMIF and not an ESCD, then the link address must be set to 1 and the LPAR parameter is used to select the logical partition.

CU address The control unit address defined in the host for the 2216. This must match the entry defined in the host IOCP CUADD parameter in the CNTLUNIT macro.

LPAR number Allows multiple partitions in a logically partitioned (LPAR) host to share one ESCON fiber. If you are using EMIF on the host, the value entered here must be the logical partition number for this connection. If you are using an ESCD, then it must be set to 1.

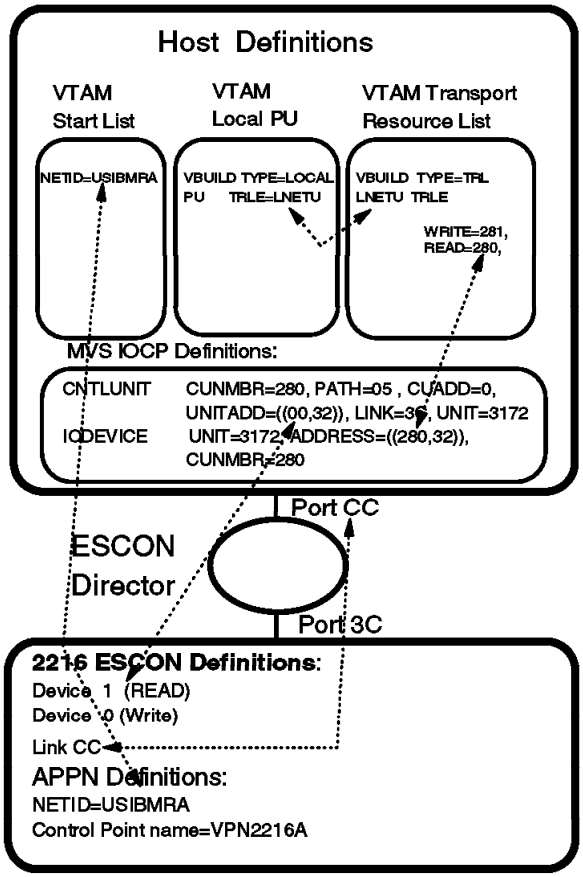


Figure 126. Host/2216 Parameter Relationships - MPC+

Notes:

1. The device addresses specified in the 2216 MPC+ interface definition must be within the range specified in the UNITADD parameter in the CNTLUNIT macro from the IOCP. For example, the UNITADD parameter in Figure 126 shows that 32 (decimal) device addresses starting at 00 (hex) are being reserved for the 2216 definition. Device addresses 00 and 01 have been specified for the 2216 MPC+ interface. Since 00 and 01 are in the range between 00 and 1F hex, this is OK as long as no other device (or interface on this 2216) tries to use these same subchannels.
2. The values specified in the VTAM TRL major node definition must be within the range specified in the ADDRESS parameter in the IODEVICE macro from the IOCP. For example, the TRL major node definition in Figure 126 specifies 280 and 281 which are in the range between 280 and 29F that the ADDRESS parameter in the IODEVICE statement specifies.
3. The values specified for the ADDRESS parameter in the IODEVICE macro and the UNITADD parameter in the CNTLUNIT macro are related *by convention only*. When defining device addresses on the 2216 MPC+ definition, use the UNITADD parameter and not the ADDRESS parameter to determine the valid range of values.

Because MPC+ operates with at least one subchannel for each direction you need to add a write subchannel address next. This step, shown in Figure 127 on page 92, is very similar to adding a read subchannel.

```
Li ESCON Add Virtual>sub addw
Li ESCON Add MPC+ Write Subchannel>device
Device address (range 0x00-0xFF): [2]? 0
Li ESCON Add MPC+ Write Subchannel>link
Link address (ESCD Port) (range 0x01-0xFE): [CC]? cc
Li ESCON Add MPC+ Write Subchannel>cu
Control Unit Logical Address (range 0x0-0xF): [0]? 0
Li ESCON Add MPC+ Write Subchannel>lpar
LPAR number (range 0x0-0xf): [1]? 1
Li ESCON Add MPC+ Write Subchannel>exit
```

Figure 127. Adding a Write Subchannel

Next, we list the subchannels that we just defined to check that we have entered the parameters correctly. This is shown in Figure 128.

```
Li ESCON Add Virtual>sub list
          Read Subchannels:
          Sub  0   Device address   :  1   LPAR number        : 1
                   Link address     : CC   CU Logical Address : 0
          Write Subchannels:
          Sub  1   Device address   :  0   LPAR number        : 1
                   Link address     : CC   CU Logical Address : 0
Li ESCON Add Virtual>exit
```

Figure 128. Listing the Configured Subchannels

Finally, we list all the interface parameters for our ESCON interface as shown in Figure 129. This shows the listing of the ESCON interface (for which we accepted the defaults) as well as the newly-defined read and write subchannels.

```
Li ESCON Config>list all
Net : 7   Protocol: MPC+   LAN type: MPC+            LAN number:  0
          Maxdata: 2048
          Reply TO : 45000   Sequencing Interval Timer: 3000
          Outbound protocol data blocking is enabled
          Block Timer:    5 ms   ACK length:   10 bytes
          Read Subchannels:
          Sub  0   Dev addr:  1  LPAR: 1  Link addr: CC  CU addr: 0
          Write Subchannels:
          Sub  1   Dev addr:  0  LPAR: 1  Link addr: CC  CU addr: 0
```

Figure 129. Listing the ESCON Interface

This completes the steps necessary to add the ESCON adapter and the MPC+ virtual interface. When you exit the ESCON configuration you will be prompted if you want to keep the changes. You must answer yes. Also, before continuing with the configuration, you need to reload the router. Figure 130 on page 93 shows these steps.

```
Li ESCON Config>exit
ESCON configuration has been changed.
Do you wish to keep the changes? [Yes]: y
Li Config>
Li *reload
Are you sure you want to reload the gateway? (Yes or [No]): yes
The configuration has been changed, save it? (Yes or No orAbort):yes
Config Save: Using bank A and config number 2
The configuration has been saved.
```

Figure 130. Reloading the Router

After the router comes back up, use the `list device` command to see the MPC virtual interface that was added in the last step. Figure 131 shows that a new MPC+ interface (interface 7) was added to our configuration.

```
Copyright Notices:

Licensed Materials - Property of IBM
Multiprotocol Access Services
(C) Copyright IBM Corp. 1997, 1998
All Rights Reserved. US Gov. Users Restricted Rights -
Use, duplication or disclosure restricted
by GSA ADP Schedule Contract with IBM Corp.


MOS Operator Control

Li *t 6
Gateway user configuration
Li Config>list dev
Ifc 0     Token Ring                        Slot: 1   Port: 1
Ifc 1     Token Ring                        Slot: 1   Port: 2
Ifc 2     Ethernet                          Slot: 5   Port: 1
Ifc 3     Ethernet                          Slot: 5   Port: 2
Ifc 4     V.35/V.36 PPP                     Slot: 6   Port: 0
Ifc 5     V.35/V.36 Frame Relay             Slot: 6   Port: 1
Ifc 6     ESCON Channel                     Slot: 3   Port: 1
Ifc 7     MPC - ESCON Channel               Base Net: 6
```

Figure 131. Checking for the MPC Interface

The next step is to add an APPN port for our new MPC+ interface. This is done from the APPN protocol menu as shown in Figure 132 on page 94.

```
Li Config>p appn
Li APPN config>add port
APPN Port
Link Type: (P)PP, (FR)AME RELAY, (E)THERNET, (T)OKEN RING,
(M)PC, (S)DLC, (X)25, (FD)DI, (D)LSw, (A)TM, (I)P  [ ]? m
Interface number(Default 0): [0]? 7
Port name (Max 8 characters) [MPC00007]?
Enable APPN on this port (Y)es (N)o [Y]?
Port Definition
Service any node: (Y)es (N)o [Y]?
Maximum BTU size (768-32768) [2048]?
Edit MPC+ Sequencing Interval Timer: (Y)es (N)o [N]?
Edit TG Characteristics: (Y)es (N)o [N]?
Edit HPR defaults: (Y)es (N)o [N]?
Write this record? [Y]?
The record has been written.
```

Figure 132. Adding an APPN Port for the MPC+ Interface

Note: You might notice that the menus do not prompt you whether to enable High Performance Routing (HPR) on this port. This is because MPC+ supports HPR only. It does not support APPN Intermediate Session Routing (ISR).

Next, we add a link station to the host. This is shown in Figure 133. The port name specified is the name of the APPN port that we created in the last step. The adjacent node type is 0 because we defined VTAM as a network node in the VTAM startup parameters.

```
Li APPN config>add link
APPN Station
Port name for the link station [ ]? mpc00007
Station name (Max 8 characters) [ ]? tovtam
Adjacent node type: 0 = APPN network node,
1 = APPN end node or Unknown node type [0]? 0
Allow CP-CP sessions on this link (Y)es (N)o [Y]?
CP-CP session level security (Y)es (N)o [N]?
Configure CP name of adjacent node: (Y)es (N)o [N]?
Edit TG Characteristics: (Y)es (N)o [N]?
Edit HPR defaults: (Y)es (N)o [N]?
Write this record? [Y]?
The record has been written.
```

Figure 133. Adding a Link to VTAM

Now we list the complete APPN configuration as shown in Figure 134 on page 95. Note that DLUR is not enabled for this node. DLUR support is not needed on the 2216. In this configuration, the 2216 is merely providing automatic network routing (ANR) services as an intermediate APPN node.

Note: DLUR is needed on the 2210 as it is that router that is providing the DLUR support for the downstream PUs in the branch. We configure DLUR for the 2210 in the next step.

From the port section in the listing, it can be seen that our new MPC+ port has been added and is enabled. In this configuration, we only make use of this port

(MPC00007) and the Enterprise Extender port (HPRIP1). The other ports, ETH0IF2 and TOWNTA, are not used in this scenario.

In the link station list, our new link station (TOVTAM) appears. This is the MPC+ connection between the 2216 and the host over the ESCON channel.

```
Li APPN config>list all
NODE :
NETWORK ID: USIBMRA
CONTROL POINT NAME: VPN2216A
XID: 00000
APPN ENABLED: YES
BREX OR BORDER NODE: NEITHER
MAX SHARED MEMORY: 5108
MAX CACHED: 4000
DLUR :
DLUR ENABLED: NO
PRIMARY DLUS NAME:
TN3270 :
TN3270E enabled: NO
TN3270E IP Address: 0.0.0.0
TN3270E Port Number: 23
CONNECTION NETWORK:
      CN NAME       LINK TYPE  PORT INTERFACES
------------------------------------------------------------
COS :
COS NAME
--------
  #BATCH
#BATCHSC
#CONNECT
  #INTER
#INTERSC
 CPSVCMG
SNASVCMG
MODE:
 MODE NAME  COS NAME
--------------------
PORT ::
  INTF     PORT      LINK      HPR    SERVICE   PORT
 NUMBER    NAME      TYPE    ENABLED    ANY    ENABLED
-----------------------------------------------------
     3    TOWNTA   ETHERAND    YES      YES      YES
 65535    HPRIP1     HPR_IP    YES      YES      YES
     2   ETH0IF2   ETHERAND    YES      YES      YES
     7  MPC00007       MPC+    YES      YES      YES
STATION :
 STATION    PORT       DESTINATION      HPR    ALLOW  ADJ NODE
  NAME      NAME         ADDRESS      ENABLED  CP-CP    TYPE
------------------------------------------------------------
 IPLINK1   HPRIP1    192.168.189.59     YES     YES       0
  TOVTAM MPC00007      000000000000     YES     YES       0
LU NAME :
      LU NAME         STATION NAME           CP NAME
------------------------------------------------------------

Li APPN config>
```

Figure 134. Listing the APPN Configuration

It is not necessary to restart the router at this point. To activate the changes to the APPN configuration, we simply issue the activate command from the APPN Config> prompt. This is illustrated in Figure 135 on page 96.

```
Li APPN config>activate
```

Figure 135. Activating the New APPN Configuration

This completes the steps necessary to configure the 2216 for this scenario.

7.1.4 Configuring the Branch Router for DLUR

In Chapter 6, “APPN through an IPSec Tunnel” on page 77, we added APPN support on the branch router specifying it as a network node and using HPR over IP to communicate to the 2216 in the data center. For this scenario, the only change necessary to the 2210 configuration is to add the DLUR support to this existing APPN configuration.

Adding DLUR support is quite simple. From the APPN configuration, we specify to enable DLUR. Then, we provide the CP name of the primary DLUS (VTAM). Finally, we activate the DLUR configuration in the router. These steps are shown in Figure 136.

```
Karen *t 6
Gateway user configuration
Karen Config>p appn
Karen APPN config>set dlur
Enable DLUR (Y)es (N)o [N]? y
Fully-qualified CP name of primary DLUS []? USIBMRA.RA03M
Fully-qualified CP name of backup DLUS []?
Perform retries to restore disrupted pipe [Y]?
Delay before initiating retries(0-2756000 seconds) [120]?
Perform short retries to restore disrupted pipe [Y]?
Short retry timer(0-2756000 seconds) [120]?
Short retry count(0-65535) [5]?
Perform long retry to restore disrupted pipe [Y]?
Long retry timer(0-2756000 seconds) [300]?
Write this record? [Y]?
The record has been written.
Karen APPN config>activate
```

Figure 136. Enabling DLUR in the Branch Router

Note: For more information about DLUR configuration, refer to the 2210 or 2216 protocol configuration and monitoring reference, volume 2.

This completes the steps necessary to configure the 2210 for DLUR support in this scenario.

7.1.5 Testing DLUR (IPSec Disabled)

At this point, the configuration of both routers and the host is complete and IPSec and the IP filters have been temporarily disabled. Now, we need to test the DLUR function before re-enabling IPSec and the packet filters.

In our scenario, we use a PC with PCOMM for OS/2 connected to the token-ring segment on the 2210. This device is configured with one 3270 session back to the host in the data center.

We first check the status of the APPN ports on the 2216. Figure 137 shows that both ports 7 and 8 are in the active (ACT_PORT) state. Remember these are the ports defined for the MPC+ connection and the HPR over IP port respectively.

```
Li *t 5

Li APPN >li port
  Intf        Name       DLC Type        HPR          State
============================================================
    8       HPRIP1         HPR_IP       TRUE       ACT_PORT
    2      ETHOIF2       ETHERAND       TRUE       ACT_PORT
    3       TOWNTA       ETHERAND       TRUE       ACT_PORT
    7     MPC00007           MPC+       TRUE       ACT_PORT
```

Figure 137. Checking the MPC+ Port Status

Next, we verify the status of the link stations on the routers. This is shown in Figure 138 for the 2216. From the figure, you can see that the MPC+ and HPR over IP links are in the active (ACT_LS) state. (Remember that IPLINK1 is our link station between the routers and TOVTAM is the link station for the MPC+ connection to the host.)

```
Li APPN >li link
    Name   Port Name  Intf       Adj CP Name  Type       HPR      State
========================================================================
 IPLINK1      HPRIP1     8  USIBMRA.VPN2210A    NN    ACTIVE     ACT_LS
  TOVTAM    MPC00007     7                      NN   ENABLED     ACT_LS
```

Figure 138. Checking the Status of the Link to VTAM

Finally, we verify that there is an APPC session between the branch router and VTAM. This is done from talk 5 by listing the active APPC sessions as shown in Figure 139 on page 98. (Remember VTAM is USIBMRA.RA03M.)

```
Karen APPN config>
Karen *t 5
Karen APPN >li appc
LU Name             Mode  Type  FSM
=====================================
USIBMRA.RAO3M     CPSVRMGR Pri  ACT
USIBMRA.RAO3M     CPSVRMGR Sec  ACT
USIBMRA.VPN2216A  CPSVCMG  Pri  ACT
USIBMRA.VPN2216A  CPSVCMG  Sec  ACT
```

Figure 139. Listing the APPC Sessions

Note: The CPSVRMGR sessions will not come up until the downstream link to PC B comes up. This triggers the DLUR to activate its DLUR-DLUS session to VTAM.

7.1.6 Re-testing DLUR with IPSec Enabled

At this point, we can re-enable IPSec and the packet filters to make certain that our configuration works through our VPN tunnel. To re-enable IPSec and access control, we use the same procedures that we used in 4.1.4, “Re-enabling Access Control and IPSec” on page 60.

After these steps have been performed, we first check the status of the defined tunnels to make sure that they are in fact enabled. This is shown in Figure 140 where you can see that our two previously defined tunnels have been re-enabled.

```
Li +f ip
Li IPsec>list all

IPsec is ENABLED

Defined Manual Tunnels:

   ID         Name         Local IP Addr   Remote IP Addr   Mode    State
 ------  ---------------  ---------------  ---------------  -----  ------
      1  ESP&AH             192.168.189.1   192.168.189.59  TUNN   Enable
      2  TRANS-ESP&AH       192.168.189.1   192.168.189.59  TRANS  Enable

Tunnel Cache:

 ID     Local IP Addr   Remote IP Addr   Mode   Policy  Tunnel Expiration
-----  ---------------  ---------------  -----  ------  -----------------
    2    192.168.189.1   192.168.189.59  TRANS  ESP-AH  11:05  Jun 20 199
    1    192.168.189.1   192.168.189.59  TUNN   ESP-AH  11:05  Jun 20 199
```

Figure 140. Checking IPSec Status

Next, we check to see that the APPC sessions are still active on the 2216. This is shown in Figure 141 on page 99.

```
Karen APPN config>
Karen *t 5
Karen APPN >li appc
LU Name             Mode  Type  FSM
====================================
USIBMRA.RAO3M     CPSVRMGR Pri  ACT
USIBMRA.RAO3M     CPSVRMGR Sec  ACT
USIBMRA.VPN2216A  CPSVCMG  Pri  ACT
USIBMRA.VPN2216A  CPSVCMG  Sec  ACT
```

Figure 141. Listing the Active APPC Sessions

Now, to make sure that the APPN traffic is actually going through the IPSec tunnel, we check the IPSec statistics to see if the counters are increasing. This is shown in Figure 142. Remember that in this case, tunnel 2 is used since that is the tunnel that HPR over IP traffic is funneled into.

```
Li IPsec>stats
Enter the Tunnel ID, Tunnel Name, or 'ALL' [ALL]? 2

                          Global IPSec Statistics
Received:
  total pkts   AH packets   ESP packets   total bytes    AH bytes     ESP bytes
  ----------   ----------   -----------   -----------   ----------   ----------
      114414       114414        114414      23581152     13163544     10417608

Sent:
  total pkts   AH packets   ESP packets   total bytes    AH bytes     ESP bytes
  ----------   ----------   -----------   -----------   ----------   ----------
         338          338           338         59968        36744        23224

Receive Packet Errors:
  total errs    AH errors   AH bad seq   ESP errors   ESP bad seq
  ----------   ----------   ----------   ----------   -----------
           0            0            0            0             0

Send Packet Errors:
  total errs    AH errors   ESP errors
  ----------   ----------   ----------
           0            0            0

Li IPsec>
```

Figure 142. Checking the IPSec Statistics

You can also check the counters on the packet filters as a way to verify that the APPN traffic is going through the IPSec tunnel. Figure 143 on page 100 shows the outbound packet filter for the 2216. Tunnel 2 uses filters 3 and 4.

```
Li IP>pac pf_out_0
Name              Dir  Intf  State  Src-Addr-Ver  #Access-Controls
pf_out_0          Out  0     On     N/A           4

Access Control currently enabled
Access Control facility: USER

Access Control run 692 times, 348 cache hits

List of access control records:

1   Type=I S   Source=192.168.180.0    Dest=192.168.157.0    Prot=  0-255
               Mask=  255.255.255.0    Mask=255.255.255.0    Use=0
               SPorts=N/A              DPorts=N/A            Tid=1
                                       Log=No

2   Type=I S   Source=9.24.105.0       Dest=192.168.157.0    Prot=  0-255
               Mask=  255.255.255.0    Mask=255.255.255.0    Use=0
               SPorts=N/A              DPorts=N/A            Tid=1
                                       Log=No

3   Type=I     Source=192.168.189.1    Dest=192.168.189.59   Prot= 50-51
               Mask=  255.255.255.255  Mask=255.255.255.255  Use=346
               SPorts=    0-65535      DPorts=    0-65535
                                       Log=No

4   Type=I S   Source=192.168.189.1    Dest=192.168.189.59   Prot=  0-255
               Mask=  255.255.255.255  Mask=255.255.255.255  Use=346
               SPorts=N/A              DPorts=N/A            Tid=2
                                       Log=No
Li IP>
```

Figure 143. Checking the Packet Filters

This completes the section for configuration and testing of DLUR through an IPSec tunnel.

Chapter 8. Adding TN3270E Server

The TN3270E Server function available in both MRS and MAS provides a gateway function for telnet 3270 clients that are downstream of a SNA host. These clients connect to the gateway using a TCP connection that is mapped to a SNA dependent LU-LU session that the gateway maintains with the SNA host. Thus, the TN3270E Server handles the conversion between the TN3270 data stream and a SNA 3270 data stream.

Figure 144 shows the configuration used to produce our TN3270E scenario.

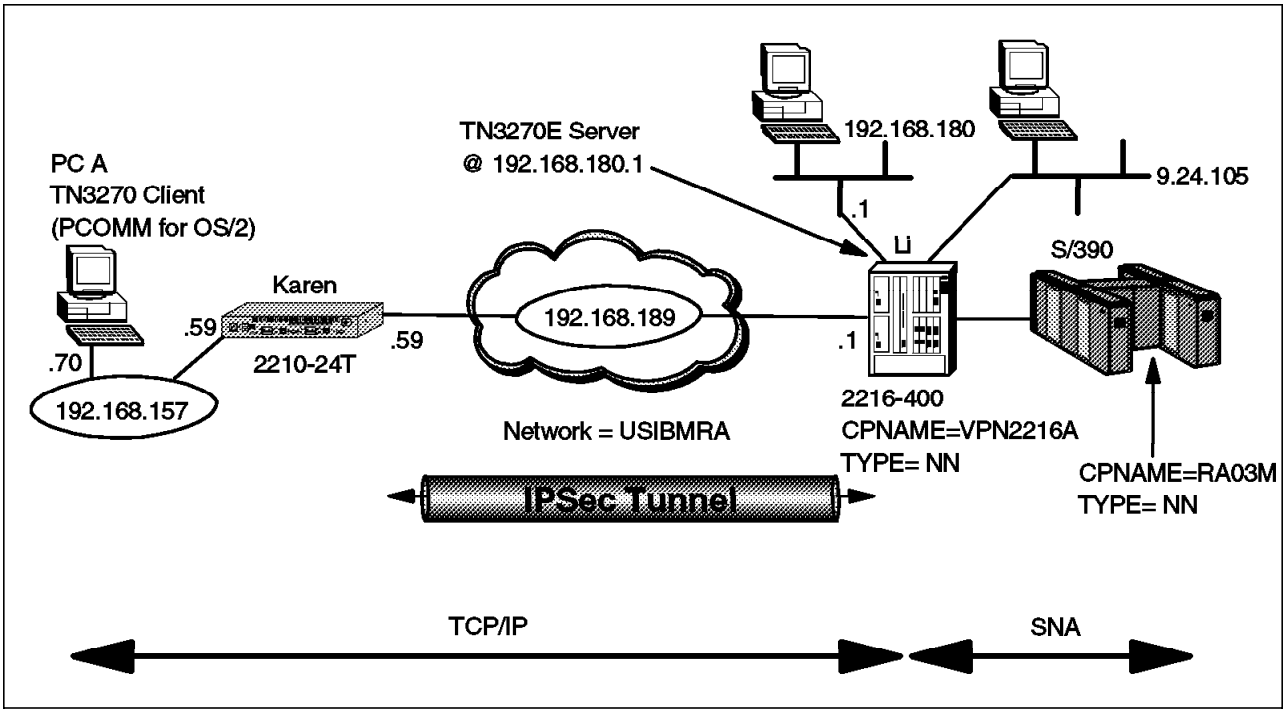


Figure 144. TN3270E through an IPSec Tunnel

In our scenario, the TN3270 clients in the branch office connect to the TN3270E Server located in the 2216 at the corporate data center. As these connections are TCP based, we use our IPSec tunnel once again to protect them.

Note: We could also configure the 2210 router in the branch as a TN3270E server (instead of putting it in the 2216). The TN3270E Server support in MRS/MAS is very flexible and allows you to make the decision to centralize or distribute this function based on your company's requirements. If we had chosen to distribute the TN3270E Server function out to the branch, the DLUR configuration would be the same as in Chapter 7, "Adding Dependent LU Requester" on page 85. The TN3270E Server would use the DLUR function configured in the branch router to communicate with the DLUS in VTAM. We would use HPR/IP through our IPSec tunnel between the two routers.

To test our configuration, we placed a PC on the branch token-ring running telnet 3270 (in PCOMM for OS/2). This PC is labeled PC A in the diagram. PC A connects to the TN3270E Server in the 2216 located in the corporate data center at IP address 192.168.180.1.

8.1 Configuring TN3270E Server in an IPSec Environment

The configuration of the 2210 router remains unchanged from that used in the basic IPSec tunnel scenario. (See Chapter 3, “Connecting the Data Center to the Branch Office” on page 33.)

For the 2216 in the data center, we start with the APPN configuration used in Chapter 6, “APPN through an IPSec Tunnel” on page 77 and we add a TN3270E server and DLUR configuration.

An MRS/MAS TN3270E Server can connect to an SNA host either by APPN or by a subarea connection (V3.1 or later). In this case, we chose to use the APPN over MPC+ connection that we defined in Chapter 7, “Adding Dependent LU Requester” on page 85.

For this configuration, the 2210 in the branch will act as a normal IP router. All TN3270 traffic between the two routers will go through the IPSec tunnel that we have configured. For example, PC A will telnet to the TN3270E Server address of 192.168.180.1. (This is an interface address on the 2216.) This TCP/IP traffic will be funneled through the IPSec tunnel 1 previously configured in Chapter 3, “Connecting the Data Center to the Branch Office” on page 33 via the inclusive access control that allows traffic from subnet 192.168.157.0 to reach subnet 192.168.180.0.

Note

This scenario was built using MRS and MAS V3.1. The talk 6 prompts for TN3270E Server changed slightly for V3.2. If you are using V3.2, the screens in this scenario will not match exactly what you see when you configure this function.

8.1.1 VTAM Definitions

As we chose APPN DLUR for the TN3270E Server to communicate with the host, we can use the same VTAM definitions that we made in Chapter 7, “Adding Dependent LU Requester” on page 85. However, we need to make additional VTAM definitions for the PUs used by the TN3270E Server. We need to make a definition for each PU in the TN3270E Server. For example, each PU in the TN3270E Server can support up to 253 LUs. If you need 500 3270 sessions, then you will need 2 PUs in the router and 2 PU definitions in VTAM.

Figure 145 on page 103 shows the host VTAM switched major node definition for the TN3270E Server PU for our scenario.

```
LOC2216  VBUILD TYPE=SWNET
M2216A   PU     ADDR=01,ISTATUS=ACTIVE,VPACING=0,                       *
                DISCNT=NO,PUTYPE=2,SSCPFM=USSSCS,USSTAB=US327X,         *
                IDBLK=077,IDNUM=02216,IRETRY=YES,MAXDATA=521,           *
                MAXOUT=7,MAXPATH=8,PASSLIM=7,PACING=0,ANS=CONTINUE
*********************************************************************
P2216A   PATH   PID=1,DLCADDR=(1,C,INTPU),DLCADDR=(2,X,07702216),       *
                DLURNAME=M2216A
*********************************************************************
JC7LU2   LU     LOCADDR=2
JC7LU3   LU     LOCADDR=3
JC7LU4   LU     LOCADDR=4
```

Figure 145. VTAM Definitions for the TN3270E Server Configuration

8.1.2 Configuring the 2216 in the Data Center

As discussed in 4.1.1, “Configuring the Data Center Router” on page 54, we make these configuration additions and test them first with the IPSec feature and IP packet filters disabled. This helps with problem determination if we experience any problems in setting up the TN3270E Server.

As a first step to configure the TN3270E Server function on the 2216, we need to add the TN3270E Server package to the router’s IPL sequence. This is shown in Figure 146. Once this command has been issued, the TN3270E Server module will be loaded during each subsequent IPL of the router.

Important Notes

You must have an MAS software load that contains the TN3270E.LD *and* the APPN.LD files in order for this work. Both APPN and subarea connectivity options for the TN3270E server require APPN support to be installed on the router. This is true even though a pure subarea configuration does not use the APPN function. This is an implementation statement as the TN3270E server function uses the APPN SNA stack for both subarea and APPN connections to the host.

```
Li *t 6

Li Config>load add package tn3270e
tn3270e package configured successfully
Li Config>
Li *reload
Are you sure you want to reload the gateway? (Yes or [No]): yes
The configuration has been changed, save it? (Yes or [No] or Abort): yes
Config Save: Using bank A and config number 3
The configuration has been saved.
```

Figure 146. Configuring the Necessary 2216 Code Modules

Note: The APPN package was already loaded. (See Figure 108 on page 78.)

After the router reloads, we go to the talk 6 APPN protocol menus and we enable DLUR and configure the primary CP name of the DLUS in VTAM. This is shown in Figure 147 on page 104.

```
Li APPN config>set dlur
Enable DLUR (Y)es (N)o [N]? y
Fully-qualified CP name of primary DLUS []? USIBMRA.RA03M
Fully-qualified CP name of backup DLUS []?
Perform retries to restore disrupted pipe [Y]?
Delay before initiating retries(0-2756000 seconds) [120]?
Perform short retries to restore disrupted pipe [Y]?
Short retry timer(0-2756000 seconds) [120]?
Short retry count(0-65535) [5]?
Perform long retry to restore disrupted pipe [Y]?
Long retry timer(0-2756000 seconds) [300]?
Write this record? [Y]?
The record has been written.
```

Figure 147. Enabling DLUR on the 2216

Next, we add a local PU on the 2216. This Local PU will be used by the TN3270E Server to establish a CP-CP session to VTAM. Note that the Local Node ID that we configure in Figure 148 is the IDNUM of the switched major node configured on VTAM. (See Figure 145 on page 103.)

```
Li APPN config>add local
Local PU information
Station name (Max 8 characters) []? M2216A
Fully-qualified CP name of primary DLUS []? USIBMRA.RA03M
Fully-qualified CP name of a backup DLUS []?
Local Node ID (5 hex digits) [00000]? 02216
Autoactivate (y/n) [Y]?
Write this record? [Y]?
The record has been written.
```

Figure 148. Configuring a Local PU

Note: Each PU can handle 253 LUs, so if we needed more than 253 LUs, we would have to define another local PU that corresponds to another VTAM switched major node with a different IDNUM value.

Next, we enable and configure the TN3270E Server. The TN3270E Server is configured from within the APPN configuration process. This is shown in Figure 149 on page 105.

```
Li APPN config>set tn3270
TN3270E Server Parameters
Enable TN3270E Server (Y/N) [N]? y
TN3270E Server IP Address []? 192.168.180.1
Port Number [23]?
Keepalive type:
 0 = none,
 1 = Timing Mark,
 2 = NOP [2]?
Frequency ( 1 - 65535 seconds) [60]?
Automatic Logoff (Y/N) [Y]?
 Time (1 - 65535 minutes)  [30]?
Enable IP Precedence (Y/N) [N]?
Write this record? [Y]?
The record has been written.
```

Figure 149. Enabling TN3270E Server

Please keep in mind the following notes when configuring the TN3270E Server:

IP Address The address that will be used by the TN3270 clients to reach the server. This address can be any interface address or the internal IP address of the router. However, keep in mind that whatever address you use for the TN3270E Server will be unavailable to use as a normal telnet to the router unless you change the port number on which the TN3270E Server listens.

> **Reminder**
>
> You must configure an IP filter that allows the TN3270E clients to access the IP address that you have defined for the TN3270E Server. In this case, from the 192.168.157.0 subnet to the 192.168.180.0 subnet. (See access control number 1 in Figure 43 on page 37.) This access control funnels the TN3270 traffic (and all other IP traffic to/from these subnets) through the IPSec tunnel.

Port Number The port number on which the TN3270E Server will listen.

Keepalive Type Whether and how the server polls clients to see if they are still active. Possible values are:

- **None** Server does not poll clients, and will only discover client absence when trying to send data.
- **NOP** Server polls clients at the TCP level. Client software need not have capability to respond.
- **Timing Mark** Server polls clients at the TN3270 level, and client software must respond within a certain time window.

Automatic Logoff Whether or not the server disconnects clients after a period of inactivity (with no data flowing in either direction).

IP Precedence This would be used, for example, if we had put the TN3270E server function on the branch router instead of the data center. It is used when the SNA traffic from/to the TN3270E Server is encapsulated in IP packets. If enabled, then the 3

precedence bits in the TOS field of the IPv4 header will be set to a value of ′011′B for all packets between the TN3270E Server and the host. This allows you to preserve your SNA priorities when using BRS even on encrypted packets. Please see the *Nways Multiprotocol Access Services Protocol Configuration and Monitoring Reference, Volume 2*, SC30-3885 for more information.

Next, we define our downstream LU resources that the clients will access. The downstream LUs can be defined either as explicit or implicit:

- Use explicit definitions when you need to ensure that the device will always use the same LU name. (For example, printers would normally use explicit definitions.)
- Use implicit definitions when you have a large group of devices that can use a common pool of available LUs and do not need to use the same LU name every time.

In Figure 150, we define an implicit pool of LUs for our TN3270E Server. We specify the station name (local PU) from which the LUs will be allocated and specify the number of LUs available in this pool.

```
Li APPN config>add tn imp
TN3270E Server LU Implicit Pool
Station name (Max 8 characters) []? m2216a
LU Name Mask (Max 5 characters) [@01LU]?
Number of Implicit LUs in Pool(1-253) [1]? 4
Write this record? [Y]?
The record has been written.
```

Figure 150. Enabling TN3270E Server

The @01LU is a template that will be used to create the actual LU names in the pool. In this example, with 4 LUs in the pool, the LU names generated are 01LU2, 01LU3, 01LU4, and 01LU5 which correspond to LOCADDRs 2-5 for the PU defined in VTAM.

Next, we list our TN3270E Server configuration as shown in Figure 151 on page 107 so that we can check our work.

```
Li APPN config>li tn
TN3270E Server Definitions
TN3270E enabled: YES
TN3270E IP Address: 192.168.180.1
TN3270E Port Number: 23
Keepalive type: NOP          Frequency: 60
Automatic Logoff: Y        Timeout: 30
Enable IP Precedence: N

DLUS Link Station: M2216A
Fully-qualified CP name of primary DLUS: USIBMRA.RAO3M
Fully-qualified CP name of backup DLUS:
Local Node ID: O2216
Auto activate : YES
Implicit Pool Information
Number of LUs: 4
LU Mask: @O1LU
LU Name   NAU addr     Class             Assoc LU Name   Assoc NAU addr
------------------------------------------------------------------------
```

Figure 151. Listing TN3270E Server Configuration

Finally, we activate our changes to the configuration as shown in Figure 152. Note that since we have already enabled APPN previously, we can just issue the activate command instead of having to reload the router.

```
Li APPN config>activate
```

Figure 152. Activating the TN3270E Server Configuration

8.1.3 Testing TN3270E Server

Now, it is time to test if the configuration is working as we intended. For this we see if there is an SSCP-LU session between the TN3270E Server and client. (We also check our TN3270 client and see if it has an active connection to the host.) From talk 5, in the APPN monitor, we issue the `list tn3270` command as shown in Figure 153 on page 108. As you can see, we have one LU that is in the active state. Since no user is logged on however, the LU is in the SSCP-LU state and not the LU-LU state.

```
Li APPN config>
Li *t 5
Li +p appn
APPN GWCON
Li APPN >li tn3270
TN3270E Server Status Summary

TN3270E IP Address: 192.168.180.1       TN3270E Port Number: 23
  Keepalive type: NOP          Frequency: 60
  Automatic Logoff: Y        Timeout: 30 minutes
  Number of connections: 1
  Number of connections in SSCP-LU state: 1
  Number of connections in LU-LU state: 0
```

Figure 153. Checking the TN3270E Server for LU Status

8.1.4 Testing TN3270E Server with IPSec Enabled

Next, we re-enable access controls and IPSec. Then, check if the TN3270E Server is still working. In Figure 154, we check the IPSec status. We see that both our tunnels as well as the IPSec feature are enabled.

```
Li +f ip
Li IPsec>list all

IPsec is ENABLED

Defined Manual Tunnels:

   ID         Name         Local IP Addr   Remote IP Addr   Mode    State
 ------  ---------------  ---------------  ---------------  -----  ------
      1  ESP&AH             192.168.189.1   192.168.189.59  TUNN   Enable
      2  TRANS-ESP&AH       192.168.189.1   192.168.189.59  TRANS  Enable

Tunnel Cache:

 ID     Local IP Addr   Remote IP Addr   Mode   Policy  Tunnel Expiration
-----  ---------------  ---------------  -----  ------  -----------------
    2    192.168.189.1   192.168.189.59  TRANS  ESP-AH  11:32  Jun 23 199
    1    192.168.189.1   192.168.189.59  TUNN   ESP-AH  11:32  Jun 23 199
Li IPsec>exit
```

Figure 154. Testing TN3270E Server with IPSec Enabled

Next, we check to make sure our TN3270E Server is still working as shown in Figure 155 on page 109.

```
Li APPN config>
Li *t 5
Li +p appn
APPN GWCON
Li APPN >li tn3270
TN3270E Server Status Summary

TN3270E IP Address: 192.168.180.1       TN3270E Port Number: 23
  Keepalive type: NOP          Frequency: 60
  Automatic Logoff: Y        Timeout: 30 minutes
  Number of connections: 1
  Number of connections in SSCP-LU state: 1
  Number of connections in LU-LU state: 0
```

Figure 155. Checking the Status of the TN3270E Server

As a double check to make sure that the TN3270 client traffic is going through the IPSec tunnel, we check the IPSec statistics to see if the counters are increasing. This is shown in Figure 156. We check tunnel number 1 this time because that is the tunnel that we specified for all traffic between the 192.168.157.0 subnet and the 192.168.180.0 subnet.

```
Li IPsec>stats
Enter the Tunnel ID, Tunnel Name, or 'ALL' [ALL]? 1

                          Global IPSec Statistics
Received:
  total pkts   AH packets   ESP packets   total bytes    AH bytes     ESP bytes
  ----------   ----------   -----------   -----------   ----------   ----------
      217533       217533        217533      33578732     31541266    7453341

Sent:
  total pkts   AH packets   ESP packets   total bytes    AH bytes     ESP bytes
  ----------   ----------   -----------   -----------   ----------   ----------
         155          155           155         10345         8978        4356

Receive Packet Errors:
  total errs    AH errors   AH bad seq   ESP errors   ESP bad seq
  ----------   ----------   ----------   ----------   -----------
           0            0            0            0             0

Send Packet Errors:
  total errs    AH errors   ESP errors
  ----------   ----------   ----------
           0            0            0

Li IPsec>
```

Figure 156. Checking IPSec Statistics

Finally, we check the IP packet filter counters to see if they are increasing as shown in Figure 157 on page 110.

```
Li IP>pac pf_out_0
Name              Dir  Intf  State  Src-Addr-Ver  #Access-Controls
pf_out_0          Out  0     On     N/A           4

Access Control currently enabled
Access Control facility: USER

Access Control run 308 times, 450 cache hits

List of access control records:

1   Type=I S   Source=192.168.180.0    Dest=192.168.157.0    Prot=  0-255
               Mask=  255.255.255.0    Mask=255.255.255.0    Use=150
               SPorts=N/A              DPorts=N/A            Tid=1
                                       Log=No

2   Type=I S   Source=9.24.105.0       Dest=192.168.157.0    Prot=  0-255
               Mask=  255.255.255.0    Mask=255.255.255.0    Use=0
               SPorts=N/A              DPorts=N/A            Tid=1
                                       Log=No

3   Type=I     Source=192.168.189.1    Dest=192.168.189.59   Prot= 50-51
               Mask=  255.255.255.255  Mask=255.255.255.255  Use=150
               SPorts=    0-65535      DPorts=    0-65535
                                       Log=No

4   Type=I S   Source=192.168.189.1    Dest=192.168.189.59   Prot=  0-255
               Mask=  255.255.255.255  Mask=255.255.255.255  Use=0
               SPorts=N/A              DPorts=N/A            Tid=2
                                       Log=No
Li IP>
```

Figure 157. Checking the Statistics for the Packet Filters

Remember that the traffic is being generated by the PC on subnet 192.168.157.0, and the TN3270E Server is at 192.168.180.1. Therefore we need to check access controls 1 and 3. Number 1 is the access control that funnels the TN3270 traffic to IPSec (traffic between subnets 192.168.157.0 and 192.168.180.0). Number 3 is the access control that allows IPSec-encrypted packets out of the router.

This completes the configuration and testing of the TN3270E Server scenario.

Chapter 9. Connecting Dial-in Remote Users

Another application of VPNs is in connecting remote dial-in users to a central site over a public IP network like the Internet. The remote access server can be administrated by an Internet Service Provider (ISP) or by the user's company itself.

In this scenario, we demonstrate how to use the IBM Nways 2210/2216 routers as Remote LAN Access (RLAN) servers using the Layer 2 Tunneling Protocol (L2TP) and Dial In Access to LANs (DIALs) features of the IBM Nways 2210/2216 routers.

The configuration that we used for this scenario is shown in Figure 158.

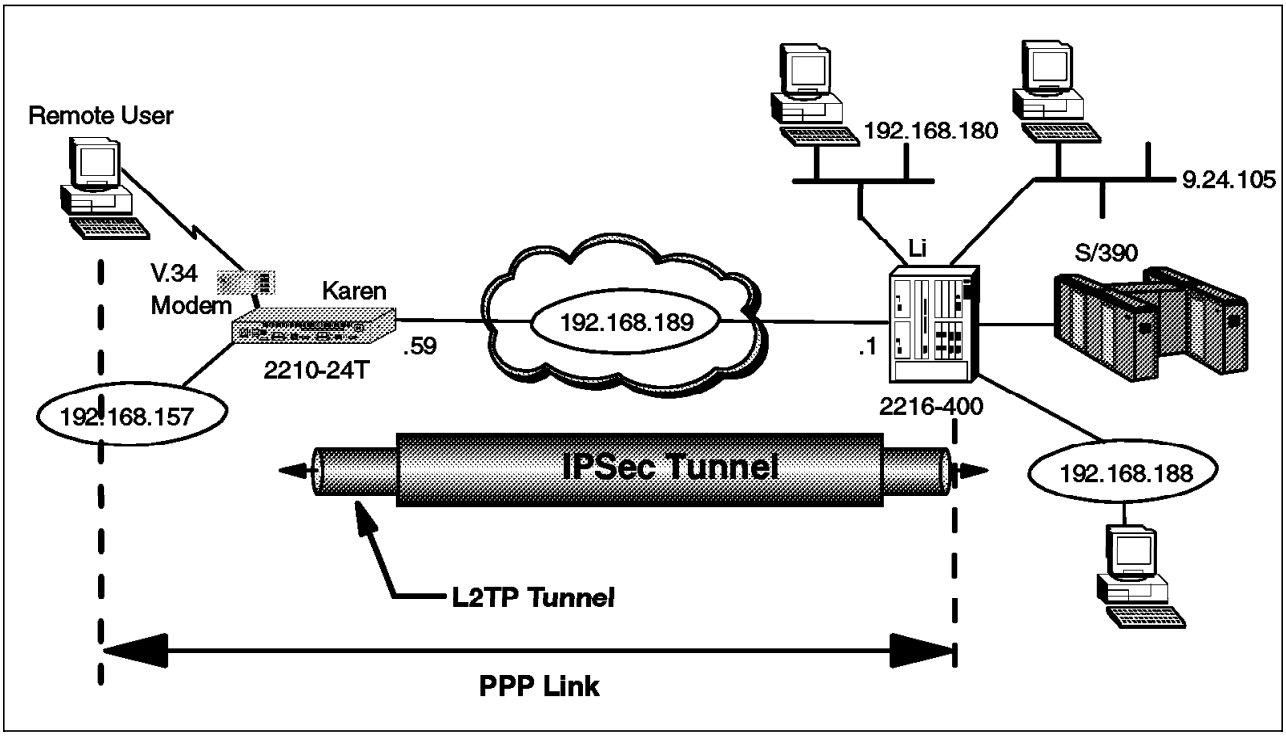


Figure 158. Tunneling an L2TP Connection through an IPSec Tunnel

For this scenario we use the same hardware configuration that we used for the previous scenarios. However, now the 2210 in the branch will also provide an RLAN server for the remote dial-in users. Also we set up a L2TP tunnel between the branch router and the 2216 in the data center so that the remote users can use the RLAN function in the 2216 to access resources on the corporate intranet.

Since the L2TP connection is IP-based, we send this traffic through the IPSec tunnel configured previously between the two routers.

9.1 Configuring the Branch Router As an RLAN Server

We start by adding a configuration to the 2210 that allows a remote user to access the LAN at his local branch via a V.34 dial-up modem.

Note: In our scenario, we demonstrate the use of V.34 for the remote user access. However, the 2210 supports V.34, ISDN BRI, and V.25bis. V.34 is

supported via external modems connected to WAN ports or via the 4- or 8-port Dial Access Adapters that provide integrated V.34 modems.

In the next part of this scenario (9.3, “Configuring L2TP in the Branch Router” on page 122), we extend the remote users′ sessions to the corporate data center location over an IP network such as the Internet by using L2TP to tunnel the PPP session from the branch-office 2210 to the central-site 2216.

Note: The IP network could be any IP-based network such as the Internet or a public frame relay network. In our scenario, the IP network is represented by an Ethernet LAN segment.

The first step in the RLAN configuration is to add a V.34 address. This is shown in Figure 159. We give it a logical name and assign a telephone number (based here on the US 10-digit numbering plan). Next, we set the data link control (DLC) protocol for WAN interface number 1 to V.34.

```
Karen *t 6
Gateway user configuration
Karen Config>add v34
Assign address name [1-23] chars []? ifv34_1
Assign network dial address [1-30 digits] []? 9193016666
Karen Config>set data v34
Interface Number [0]? 1
Karen Config>list dev
Ifc 0     Token Ring                    CSR 6000000, vector 95
Ifc 1     V.34 Base Net                 CSR  81600, CSR2  80C00, vector 94
Ifc 2     WAN PPP                       CSR  81620, CSR2  80D00, vector 93
Ifc 3     WAN PPP                       CSR  81640, CSR2  80E00, vector 92
Ifc 4     WAN PPP                       CSR  81660, CSR2  80F00, vector 91
Ifc 5     Token Ring                    CSR 6000100, vector 90
Ifc 6     NULL Device                   CSR      0, vector 0
```

Figure 159. Adding a V.34 Address and Setting the WAN Interface to V.34

As can be seen from the figure, when we list the devices, we see that WAN interface number 1 has been changed from the default DLC of PPP to V.34.

The next step is to configure the V.34 interface. This is shown in Figure 160.

```
Karen Config>net 1
V.34 Data Link Configuration
Karen V.34 System Net Config   1>set local
Local network address name   []? ifv34_1
Karen V.34 System Net Config   1>set speed
Line speed (2400 to 460800) [57600]? 57600
```

Figure 160. Configuring the V.34 Interface

All that is really necessary here is to map the V.34 port to the V.34 address created in Figure 159 and set up the baud rate of the connection. You can also set the modem initialization string, but in this environment we use the default parameters.

You can check the parameters that you configured with the `list all` command as shown in Figure 161 on page 113.

```
Karen V.34 System Net Config   1>list all

         V.34 System Net Configuration:

Local Network Address Name    = ifv34_1
Local Network Address         = 9193016666

Non-Responding addresses:
Retries                       = 1
Timeout                       = 0 seconds

Call timeouts:
Command Delay                 = 0 ms
Connect                       = 60 seconds
Disconnect                    = 2 seconds

Modem strings:
Initialization string         = AT&S1L1&D2&C1X3

Speed (bps)                   = 57600

Karen V.34 System Net Config   1>exit
```

Figure 161. Listing the Configuration of the V.34 Port

The next step is to create the virtual interfaces used for dial-in connections. RLAN users use a special kind of dial circuit called a *dial-in* circuit (as opposed to the normal dial circuit that a router uses to dial another router). For this scenario we create one virtual interface for our single RLAN test user.

Note: Though we only use one V.34 interface we could create many more. The practical limit is the number of async ports available on the router. We would do precisely the same steps for each V.34 interface available.

The dial-in interfaces are added from the talk 6 `Config>` prompt as shown in Figure 162 on page 114.

```
Karen Config>add dev dial-in
Enter the number of PPP Dial-in Circuit interfaces [1]? 1
Adding device as interface 7
Base net for this circuit [0]? 1
Defaulting Data-link protocol to PPP
Use "net <intf #>" command to configure circuit parameters

Karen Config>list dev
Ifc 0     Token Ring                    CSR 6000000, vector 95
Ifc 1     V.34 Base Net                 CSR  81600, CSR2  80C00, vector 94
Ifc 2     WAN PPP                       CSR  81620, CSR2  80D00, vector 93
Ifc 3     WAN PPP                       CSR  81640, CSR2  80E00, vector 92
Ifc 4     WAN PPP                       CSR  81660, CSR2  80F00, vector 91
Ifc 5     Token Ring                    CSR 6000100, vector 90
Ifc 6     NULL Device                   CSR      0, vector 0
Ifc 7     PPP Dial-in Circuit
```

Figure 162. Creating the Virtual Dial-in Interfaces

Note: Only PPP is supported over V.34. However, with DIALs, we can support multiple protocols (IP, IPX, NetBIOS, 802.2, and LLC) over the PPP connection.

As you can see from the `list devices` command above, the software assigns an interface number to each virtual device. We use this interface number to configure the interface.

The next step is to configure the virtual interfaces. For each dial-in circuit, there are a number of parameters which can be configured; however, these can generally be left at their default values. You can list the default parameters with the `list all` command from the configuration prompt for the interface. An example is shown in Figure 163 for the virtual interface number 7.

```
Karen Config>n 7
Circuit configuration
Karen Circuit config:   7>list all

Base net                        = 1
Destination name                = default_address
Circuit priority                = 8
Destination address:subaddress = 9999999

Inbound dst name                = * ANY *
Outbound calls                  = allowed
Inbound calls                   = allowed
Idle timer                      = 0 (standard circuit)
SelfTest Delay Timer            = 150 ms
LIDs used                       = No

Karen Circuit config:   7>
```

Figure 163. Listing the Virtual Dial-in Interface Parameters

The following is a description of these parameters:

- Idle timer

This parameter generally has no meaning as the inactivity timeout is defined globally, not per interface.

- Inbound calls

  This means that any PPP user is allowed to call. (We could reserve this circuit for a specific user, if required.)

- Outbound calls

  This does not mean that dial-in circuits can be used for dial-out. This allows a client to be called back, or when connecting via ISDN, allows PPP multilink to form a bundle of multilink channels between the dial-in client and the router.

- Default destination address.

  A default destination address of ″default-address″ is set up when the dial-in circuit is created. Because these circuits service inbound calls only, and the only outbound calls will be the result of either a callback or a multilink PPP exchange, the destination address is meaningless in this instance. However, the address is required by the software to define the circuit parameters. Do not delete this address or the circuits will come up disabled.

In addition to the parameters for the virtual interface itself, you can also configure the parameters used for the PPP encapsulator for that interface. This is done so that the parameters used at the router will match those used by the dial-in clients. While most of these parameters can be negotiated between the two ends of the PPP link at link activation time, the less negotiation that is necessary, the faster the link will come up.

The prompt for configuring the encapsulator is a sub-menu of the dial-in interface configuration prompt. In Figure 164, we show the default options for the encapsulator using the `list lcp options` command from the encapsulator sub prompt.

```
Karen Circuit config:   7>encap
Point-to-Point user configuration
Karen PPP 7 Config>list lcp options

LCP Parameters
--------------
Config Request Tries:              20   Config Nak Tries:                  10
Terminate Tries:                   10   Retry Timer:                     3000

LCP Options
-----------
Max Receive Unit:                1522   Magic Number:                      Yes
Peer to Local (RX) ACCM:        A0000
Protocol Field Comp(PFC):          Yes   Addr/Cntl Field Comp(ACFC):       Yes


Authentication Options
----------------------
Authenticate remote using:  SPAP or CHAP or PAP  [Listed in priority order]
CHAP Rechallenge Interval:  0
Identify self as:           2210out
```

Figure 164. Listing the PPP LCP Options

The MRU size can be negotiated by the router with the client. The setting in the router must be at least as large as that on the client. An MRU size of 1522 is needed for the Windows 3.1, OS/2 and DOS versions of the IBM DIALs client. Do not change the default value if one of these clients is being used.

The following notes pertain to the LCP authentication options configured for RLAN:

- SPAP, CHAP and PAP are enabled by default. The router will negotiate with the client in the order that they are listed.
- You must have at least one authentication method enabled on the interface and the client must be configured to use a method that you have enabled on the router.
- The Shiva Password Authentication Protocol (SPAP) allows the clients to change their own password in the router′s local authentication database. If you overwrite the router′s configuration (for example using the MRS graphical configuration tool), then these password changes will be lost. You can avoid this by reading the router configuration into the router before making the changes and writing the new configuration back to the router.

The next step is to define a PPP user on the 2210 so that we can test it as an RLAN server. The user will be authenticated at the 2210 when he dials in. This is shown in Figure 165 on page 117.

```
Karen Config>add ppp
Enter name:  []? kacir
Password:
Enter again to verify:
Allow inbound access for user? (Yes, No): [Yes]
Will user be tunneled? (Yes, No): [No]
Is this a 'DIALs' user? (Yes, No): [Yes]
Type of route?  (hostroute, netroute): [hostroute]
IP address: [0.0.0.0]? 192.168.157.40
Give user default time allotted ? (Yes, No): [Yes]
Enable callback for user?(Yes, No): [No]
Will user be able to dial-out ? (Yes, No): [No]
Enable encryption for this user/port (y/n) [No]:
Disable user ? (Yes, No): [No]


     PPP user name: kacir
            Expiry: <unlimited>
   User IP address: 192.168.157.40
     Netroute Mask: 255.255.255.255
          Hostname: <undefined>
      Time alotted: Box Default
     Callback type: disabled
          Dial-out: disabled
        Encryption: disabled
            Status: enabled
    Login Attempts: 0
    Login Failures: 0
  Lockout Attempts: 0

Is information correct? (Yes, No, Quit): [Yes]

User 'kacir' has been added
```

Figure 165. Creating an PPP User Continuation

The following notes pertain to adding PPP users for the DIALs function:

Notes:

1. For the first part of this scenario, the user is not tunneled. It is just a straight DIALs scenario at this point. In the next part, we specify that the user is tunneled which is the indication to the router to start an L2TP tunnel to the 2216.
2. The client's IP address is on the same subnet as the destination LAN to which he wishes to connect.
3. Configuring an IP address here means that the IP address will be provided by the user ID to the client. If you leave the IP address at 0.0.0.0, the IP address can be provided by the interface, client or DHCP server.
4. If you enable callback for the user you will be prompted to choose what type of callback you want to use.

Note.

For our scenario, we first configure the RLAN function in the branch router so that we can test the dial-in client connecting to the branch office LAN. If you are configuring only the L2TP function so that your clients will tunnel through the branch router and never use the RLAN functions in that router, then the remaining steps are not required on the branch router.

The next step is to define which method we want to use for the clients to obtain an IP address. Remote users dialing into the DIALs server (2210) need to be assigned an IP address that is on the same subnet as the LAN interface to which they wish to connect. There are five methods available:

- Client

  The IP address is configured on the client.

- User ID

  The IP address is configured as part of the User ID definition on the router and sent to the client when it is authenticated. In this case the IP address is associated with a specific user.

- Interface

  The IP address is configured in the interface and sent to the client. Here, the IP address is associated with the interface instead of the User ID.

- DHCP proxy

  The IP address will be provided by a DHCP server and the router acts as a DHCP proxy for the client.

- IP Pool

  MRS/MAS V3.2 introduces a new method called IP pooling that allows you to set up a block of IP addresses that are stored in a pool. When a client connects and requests an IP address, the router retrieves an address from the pool. The command to configure an IP pool is `add ip-pool` and it is issued from the `DIALs config>` prompt.

The methods are configured from the global DIALs menu as shown in Figure 166. In our scenario, we use the default settings of the client, user ID and interface methods enabled. The router will attempt to use the first method that is enabled (in the order that is listed).

```
Karen Config>f dial
Dial-in Access to LANs global configuration
Karen DIALs config>li ip
DIALs client IP address specification:
Client     :  Enabled
UserID     :  Enabled
Interface  :  Enabled
Pool       :  Enabled
DHCP Proxy :  Disabled
Karen DIALs config>exit
Karen Config>
```

Figure 166. Listing Methods to Obtain IP Addresses

You can also define primary and secondary domain name servers whose addresses are passed to the client during the IPCP negotiations.

In order to route IP through the V.34 interface, an IP address must be assigned to the interface. When the client dials in, the router automatically adds a static route to its routing table that says the next hop for the remote user is the IP address of the V.34 virtual interface.

The address must be on a different subnet from the destination LAN segment. You can use a real IP address or use unnumbered IP. For unnumbered IP, the format of the address is 0.0.0.n where n is the interface number (for example, for interface 7, the unnumbered IP address would be 0.0.0.7). Figure 167 shows the dialog used for our scenario. Interface 7 is our virtual interface for our test dial-in user.

```
Karen Config>p ip
Internet protocol user configuration
Karen IP config>list add
IP addresses for each interface:
   intf     0   192.168.189.59   255.255.255.0    Local wire broadcast, fill 1
   intf     1                                     IP disabled on this interface
   intf     2                                     IP disabled on this interface
   intf     3                                     IP disabled on this interface
   intf     4                                     IP disabled on this interface
   intf     5   192.168.157.59   255.255.255.0    Local wire broadcast, fill 1
   intf     6                                     IP disabled on this interface
   intf     7                                     IP disabled on this interface
Internal IP address: 192.168.189.59

Karen IP config>add address
Which net is this address for [0]? 7
New address []? 0.0.0.7
Address mask [0.0.0.0]? 255.255.255.0
```

Figure 167. Configuring IP Addresses on the Virtual Interfaces

ARP-subnet routing must be enabled in order to allow the router to respond to ARPs when the next hop to the destination is over a different interface from the interface that is receiving the ARP request. This is the case with RLAN where the client IP address is on the same subnet as the router's LAN interface but the next hop (the V.34 interface) is on a different subnet. ARP-subnet routing is enabled as shown in Figure 168 on page 120 where we also list our IP addresses to double check our latest addition.

```
Karen IP config>en arp
Karen IP config>list add
IP addresses for each interface:
   intf     0   192.168.189.59   255.255.255.0    Local wire broadcast, fill 1
   intf     1                                     IP disabled on this interface
   intf     2                                     IP disabled on this interface
   intf     3                                     IP disabled on this interface
   intf     4                                     IP disabled on this interface
   intf     5   192.168.157.59   255.255.255.0    Local wire broadcast, fill 1
   intf     6                                     IP disabled on this interface
   intf     7   0.0.0.7          255.255.255.0    Local wire broadcast, fill 1
Internal IP address: 192.168.189.59
Karen IP config>exit
```

Figure 168. Enabling ARP-Subnet Routing

This completes the configuration of the branch router for the basic DIALs function. We restart the router to activate the changes as shown in Figure 169.

```
Karen Config>
Karen *r
Are you sure you want to restart the gateway? (Yes or [No]): yes
```

Figure 169. Restarting the Router

9.2 Testing RLAN on the Branch Router

RLAN operation can be confirmed by dialing in from a remote user (using DIALs Client software on a PC) via a V.34 modem. The user should be able to test IP connectivity by pinging the target LAN interface and connecting to any device on that LAN. As this is a multiprotocol connection, other protocols (SNA, NetBIOS) can also be tested.

While there is no specific subsystem in ELS to monitor RLAN connections, there are a number of ways in which correct operation can be confirmed. One way is to monitor inbound calls from ELS (V.34) as shown in Figure 170 on page 121.

```
*t 5
>ev
ELS>nodisp sub all all
ELS>disp sub ip all
ELS>disp sub v34
ELS>
*flush 2
*talk 2

18:54:59   GW.021: Nt up nt 7 int PPP/3
18:55:00   IP.025: add nt 192.168.157.40 rt via 0.0.0.7 nt 7 int PPP/3
18:55:00   IP.068: routing cache cleared
```

Figure 170. Monitoring V.34 Inbound Calls

From the message GW.021, we see when the user dials in and we also see that interface 7 has been allocated to this call.

From the message IP.025, we can see the router adding the static route to the client IP address via the unnumbered address that we assigned to interface 7.

We can also check the state of the PPP link using the `list connection lcp` command under talk 5 for the dial-in interface. From here, we can see the LCP state, the remote user name, the time connected and the LCP options being used by both the local and remote ends of the link. This is shown in Figure 171.

```
Karen +n 7
Point-to-Point Console
Karen PPP 7>li con lcp

Version:                    1
Link phase:                 Ready for network traffic (NCP)
LCP State:                  Open
Previous State:             Ack Sent
Time Since Change:          2 minutes and 29 seconds
Remote Username:            kacir
Last Identification Rx'd
Time Connected:             2 minutes and 29 seconds

LCP Option                  Local                       Remote
----------                  -----                       ------
Max Receive Unit:           1500                        1500
Async Char Mask:            A0000                       A0000
Authentication:             C223 (CHAP)                 None
Magic Number:               C6504AB8                    2795AB71
Protocol Field Comp:        Yes                         Yes
Addr/Cntl Field Comp:       Yes                         Yes
32-Bit Checksum:            No                          No
Endpoint Discriminator:     No                          No
Rcv Short Sequence Nums:    -                           -
Link Discriminator:         0                           0
MRRU:                       0                           0
Karen PPP 7>exit
```

Figure 171. Monitoring the Dial-in Interface

Note: This command can be very useful when you want to compare the LCP options being used at each end during the startup of a new connection.

We can also check the IP route table to see whether the router dynamically created a static route to the client for the virtual PPP interface. This is shown in Figure 172.

```
Karen +p ip
Karen IP>dump
Type   Dest net         Mask      Cost     Age       Next hop(s)

Stat*  0.0.0.0          00000000  1        223       192.168.189.1
 Dir*  192.168.157.0    FFFFFF00  1        156       TKR/1
Stat*  192.168.157.40   FFFFFFFF  1        173       PPP/3
 Dir*  192.168.189.0    FFFFFF00  1        223       TKR/0

Default gateway in use.
Type Cost     Age       Next hop
Stat 1        223       192.168.189.1

Routing table size: 768 nets (52224 bytes), 4 nets known
                    0 nets hidden, 0 nets deleted, 0 nets inactive
                    0 routes used internally, 764 routes free
```

Figure 172. Monitoring the IP Route Table

From the routing table, we see that the static route has been added to our dial-in client on PPP interface 3 which is the fourth PPP interface on the box and correlates to net 7 (see Figure 162 on page 114).

9.3 Configuring L2TP in the Branch Router

Now that we have tested the DIALs function in the local branch router, we extend the dial-in user's PPP connection by setting up an L2TP tunnel between the 2210 in the branch location and 2216 in the data center. The end user should then be able to use the RLAN function in the 2216 to connect to resources in the data center. Since L2TP tunnels PPP over UDP, we can secure these packets with IPSec.

L2TP is a mechanism that involves a tunnel between an L2TP Access Concentrator (LAC) and an L2TP Network Server (LNS). In our scenario, the 2210 in the branch will be configured as the LAC and the 2216 will be configured as the LNS.

The first step is to create a tunnel in the LAC. This is shown in Figure 173 on page 123.

```
Karen Config>add tunnel
Enter name:  []? lns.org
Enter hostname to use when connecting to this peer: []? lac.org
set shared secret? (Yes, No): [No] yes
Shared secret for tunnel authentication:
Enter again to verify:
Tunnel-Server endpoint address: [0.0.0.0]? 192.168.189.1

       Tunnel name: lns.org
          Endpoint: 192.168.189.1
          Hostname: lac.org

User 'lns.org' has been added
```

Figure 173. Creating a Tunnel in the LAC

The following notes pertain to the LAC tunnel configuration:

Notes:

1. Tunnel name

   This name should match the hostname which is configured on the LNS (2216).

2. Hostname

   This is the hostname of the LAC.

3. Tunnel-Server endpoint

   The IP address of the endpoint of the tunnel. This address has to be reachable from the LAC. It can be any interface address or an internal IP address on the 2216. Here we use the address of the interface which is the endpoint of the tunnel.

   Note: Remember that in this case, the IP traffic is generated by the router. So we need to have packet filters configured to allow packets to and from the IPSec tunnel endpoints. We already configured the tunnel and the access controls for our router-to-router traffic in our previous configuration (see 3.1.1, “Configuring the Branch Office Router” on page 34).

4. Shared secret

   This parameter must be set if authentication is to be used on the tunnel and the value here must match the value configured in the LNS. L2TP tunnel authentication is enabled by default.

Next, we enable L2TP. This is shown in Figure 174 on page 124. Also, we restart the router in order to activate these changes.

```
Karen Config>f layer
Karen Layer-2-Tunneling Config>en l2tp

 Restart system for changes to take effect.
Karen Layer-2-Tunneling Config>exit
Karen Config>
Karen *r
Are you sure you want to restart the gateway? (Yes or [No]): yes
```

Figure 174. Enabling L2TP in the LAC (Branch Router)

9.4 Configuring L2TP in the 2216

Now we configure the 2216 as an L2TP Network Server (LNS). We first create the tunnel in the LNS, pointing to the IP address and the name of the LAC. This is shown in Figure 175.

```
Li *t 6
Gateway user configuration
Li Config>add tunnel
Enter name:  []? lac.org
Enter hostname to use when connecting to this peer: []? lns.org
set shared secret? (Yes, No): [No] yes
Shared secret for tunnel authentication:
Enter again to verify:
Tunnel-Server endpoint address: [0.0.0.0]? 192.168.189.59

       Tunnel name: lac.org
          Endpoint: 192.168.189.59
          Hostname: lns.org

User 'lac.org' has been added
```

Figure 175. Creating a Tunnel in the LNS

Note: If you are using shared secrets, the key here must match the one configured in the LAC.

You can modify the PPP parameters for the L2TP tunnel. However, these parameters will be negotiated between the LAC and the LNS. The LAC acts as a proxy for the client PC in the PPP negotiation. Note that an authentication protocol must be enabled for the L2TP tunnel. Figure 176 on page 125 shows a listing of the default PPP parameters on the LNS. None of these parameters needs to be changed for our scenario.

```
Li Layer-2-Tunneling Config>encap
Point-to-Point user configuration
Li PPP-L2TP Config>list all

Disabled as a Multilink PPP Link


LCP Parameters
--------------
Config Request Tries:               20   Config Nak Tries:                  10
Terminate Tries:                    10   Retry Timer:                     3000

LCP Options
-----------
Max Receive Unit:                 2048   Magic Number:                     Yes
Peer to Local (RX) ACCM:         A0000
Protocol Field Comp(PFC):           No   Addr/Cntl Field Comp(ACFC):        No

Authentication Options
----------------------
Authenticate remote using:  SPAP or CHAP or PAP  [Listed in priority order]
CHAP Rechallenge Interval:  0
Identify self as:           ibm


NCP Parameters
Config Request Tries:               20   Config Nak Tries:                  10
Terminate Tries:                    10   Retry Timer:                     3000


Dial-in Access to LANs ENABLED




CCP Options
-----------
Data Compression disabled
Algorithm list: none
STAC histories: 1
STAC check_mode: SEQ


ECP Options
-----------
Data Encryption disabled
Algorithm list: DES
DESE (Data Encryption Standard Encryption Protocol)

BCP Options
-----------
Tinygram Compression:         Disabled


IPCP Options
------------
IPCP Compression:                 None
Send Our IP Address:                No
Remote IP Address to Offer if Requested: None
Li PPP-L2TP Config>
```

Figure 176. Listing PPP Parameters for L2TP Connections

Next, we enable L2TP in the LNS as shown in Figure 177 on page 126.

```
Li Config>f layer
Li Layer-2-Tunneling Config>en l2tp

 Restart system for changes to take effect.
```

Figure 177. Enabling L2TP in the LNS

Next, we add the virtual interfaces over which the PPP connections will be terminated. These are analogous to the dial-in interface that we added in the branch router when we configured it for the DIALs function. Except in this case, the users are coming in through an L2TP tunnel instead of a V.34 interface.

In the LNS, these are added from the L2TP feature configuration prompt. (In the LAC, they were added from the talk 6 main prompt.) This is shown in Figure 178.

```
Li Layer-2-Tunneling Config>add l2
Additional L2 nets:  [0]? 3
Add unnumbered IP addresses for each L2 net? [Yes]:
Adding device as interface 8
Defaulting data-link protocol to PPP
Adding device as interface 9
Defaulting data-link protocol to PPP
Adding device as interface 10
Defaulting data-link protocol to PPP
Enable IPX on L2TP interfaces?(Yes or [No]):
Enable transparent bridging on L2TP interfaces?(Yes or [No]):
Bridge configuration was not changed.

Restart router for changes to take affect.
Li Layer-2-Tunneling Config>exit
Li Config>
```

Figure 178. Adding the Virtual Interfaces

In order to route IP through the L2 nets, an IP address must be assigned to the interface. When the client establishes the PPP connection through the L2TP tunnel, the router automatically adds a static route to its routing table that says that the next hop for the remote user is the IP address of the L2TP virtual interface. The address must be on a different subnet from the destination LAN segment.

The IP addresses for these interfaces are added when you create the interfaces. By default, they are unnumbered IP addresses. The format of the address is 0.0.0.n where n is the interface number (for example, for interface 8, the unnumbered IP address would be 0.0.0.8).

Note: If you need to change the default IP address associated with an L2TP net, you can do so via the IP config prompt in talk 6. However, unnumbered IP addressing works very well for RLAN because users connect to an L2TP net arbitrarily and the particular IP address associated with an L2TP net is not very critical.

ARP-subnet routing must be enabled in order to allow the router to respond to ARPs when the next hop to the destination is over a different interface from the interface that is receiving the ARP request. This is the case with RLAN where the client IP address is on the same subnet as the router's LAN interface but the next hop (the L2TP virtual interface) is on a different subnet. ARP-subnet routing is enabled as shown in Figure 179.

```
Li config>p ip
Li IP config>en arp
Li IP config>exit
Li config>
```

Figure 179. Enabling ARP-Subnet Routing

The next step is to define which method we want to use for the clients to obtain an IP address. In this regard, the DIALs server in the 2216 needs to be configured just as if the users were dialing in via ISDN or V.34 rather than tunneling in through an L2TP tunnel. The steps that are necessary are identical to the ones that we performed for the branch router.

DIALs users need to be assigned an IP address that is on the same subnet as the LAN interface to which they wish to connect. There are five methods available:

- Client

  The IP address is configured on the client.

- User ID

  The IP address is configured as part of the User ID definition on the router and sent to the client when it is authenticated. In this case the IP address is associated with a specific user.

- Interface

  The IP address is configured in the interface and sent to the client. Here, the IP address is associated with the interface instead of the User ID.

- DHCP Proxy

  The IP address will be provided by a DHCP server and the router acts as a DHCP proxy for the client.

- IP Pool

  MRS/MAS V3.2 introduces a new method called IP pooling that allows you to set up a block of IP addresses that are stored in a pool. When a client connects and requests an IP address, the router retrieves an address from the pool. The command to configure an IP pool is `add ip-pool` and it is issued from the `DIALs config>` prompt.

The methods are configured from the global DIALs menu as shown in Figure 180 on page 128. In our scenario, we use the default settings of the client, user ID and interface methods enabled. The router will attempt to use the first method that is enabled (in the order that is listed).

```
Li Config>f dial
Dial-in Access to LANs global configuration
Li DIALs config>li ip
DIALs client IP address specification:
Client     :  Enabled
UserID     :  Enabled
Interface  :  Enabled
Pool       :  Enabled
DHCP Proxy :  Disabled
Li DIALs config>exit
Li Config>
```

Figure 180. Listing Methods to Obtain IP Addresses

You can also define primary and secondary domain name servers whose addresses are passed to the client during the IPCP negotiations.

At this point we have the tunnel configured in both the LNS and LAC and the DIALs feature has been configured in the LNS.

Note: The DIALs feature is also configured in the LAC, but this was because we wanted to use the branch router as an RLAN server also. If we had just wanted to use it to tunnel users over to the LNS, then configuring the DIALs function in the branch router would not have been necessary.

Now we configure the PPP users that will tunnel to the LNS. There are two ways to configure the PPP users to be tunneled:

- Rhelm-Based Tunneling

  Using this method, you only need to define the user at the LNS. You must use the format username@domain where domain is the hostname of the LNS. When the client dials into the LAC using the username@domain format (for example, Steven@lns.org), the LAC will create a tunnel to the specified domain (lns.org) and the PPP connection will be tunneled to the desired destination. With this method, all users with the same domain name are tunneled to the same destination.

- User-Based Tunneling

  With this method, the user's profile has to be configured at both the LAC and the LNS, and does not use the username@domain format. In the LAC you specify, in the user's profile, where the end destination is. In the LNS, you configure a normal dial-up user.

Figure 181 on page 129 shows the definition of a Rhelm-based user on the 2216 in the data center.

```
Li Config>add ppp
Enter name:  []? steven@lns.org
Password:
Enter again to verify:
Allow inbound access for user? (Yes, No): [Yes]
Will user be tunneled? (Yes, No): [No]
Is this a 'DIALs' user? (Yes, No): [Yes]
Type of route?  (hostroute, netroute): [hostroute]
IP address: [0.0.0.0]?
Give user default time allotted ? (Yes, No): [Yes]
Enable callback for user? (Yes, No): [No]
Enable encryption for this user/port (y/n) [No]:
Disable user ? (Yes, No): [No]


     PPP user name: steven@lns.org
           Expiry: <unlimited>
   User IP address: Interface Default
     Netroute Mask: 255.255.255.255
          Hostname: <undefined>
      Time alotted: Box Default
     Callback type: disabled
        Encryption: disabled
            Status: enabled
    Login Attempts: 0
    Login Failures: 0
  Lockout Attempts: 0

Is information correct? (Yes, No, Quit): [Yes]

User 'steven@lns.org' has been added
```

Figure 181. Adding a Rhelm-Based L2TP User

For user-based tunneling, we define the ID in both the LAC and LNS. Figure 182 shows the definition of a user-based ID on the 2210 in the branch office.

```
Karen Config>add ppp
Enter name:  []? garth
Password:
Enter again to verify:
Allow inbound access for user? (Yes, No): [Yes]
Will user be tunneled? (Yes, No): [No] yes
Enter hostname to use when connecting to this peer: []? lac.org
Tunnel-Server endpoint address: [0.0.0.0]? 192.168.189.1

     PPP user name: garth
          Endpoint: 192.168.189.1
          Hostname: lac.org

Is information correct? (Yes, No, Quit): [Yes]

User 'garth' has been added
```

Figure 182. Adding a User-Based Tunneling User in the 2210 (LAC)

We define this user to be tunneled which is the router's notification to set up the L2TP tunnel when this user dials in. We then specify the destination IP address of the other tunnel endpoint as well as the hostname of the 2210 to use when creating the tunnel.

Note: As soon as we specify that this user will be tunneled, the router knows enough not to ask us about whether we want the DIALs function enabled for this user, what the IP address of the client should be, or any of the other parameters that you are prompted for when defining a DIALs user. This is because the DIALs function for this user is being provided by the 2216. The 2210 is merely providing a gateway service to the 2216.

Figure 183 shows the definition of the same user-based ID on the 2216 in the data center. Here, we define a normal DIALs user. This user is not a tunneled user because by the time he is authenticated by the DIALs function, the L2TP headers have all been stripped off and the packets are just normal PPP packets.

```
Li Config>add ppp
Enter name:  []? garth
Password:
Enter again to verify:
Allow inbound access for user? (Yes, No): [Yes]
Will user be tunneled? (Yes, No): [No] no
Is this a 'DIALs' user? (Yes, No): [Yes]
Type of route?  (hostroute, netroute): [hostroute]
IP address: [0.0.0.0]?
Give user default time allotted ? (Yes, No): [Yes]
Enable callback for user? (Yes, No): [No]
Enable encryption for this user/port (y/n) [No]:
Disable user ? (Yes, No): [No]
           PPP user name: garth
            Expiry: <unlimited>
   User IP address: Interface Default
     Netroute Mask: 255.255.255.255
          Hostname:
     Time allotted: Box Default
     Callback type: disabled
        Encryption: disabled
            Status: enabled
    Login Attempts: 0
    Login Failures: 0
  Lockout Attempts: 0

Is information correct? (Yes, No, Quit): [Yes]

User 'garth' has been added
```

Figure 183. Adding a Users Based Tunneling User in the 2216 (LNS)

This completes the configuration of the LNS. We need to reload the 2216 in order to activate these changes. This is shown in Figure 184 on page 131.

```
Li *reload
Are you sure you want to reload the gateway? (Yes or [No]): yes
The configuration has been changed, save it? (Yes or [No] or Abort): yes
Config Save: Using bank A and config number 2
The configuration has been saved.
```

Figure 184. Reloading the 2216 (LNS)

9.5 Testing L2TP (IPSec Disabled)

Now that we have the configuration in place, we test the L2TP and RLAN configuration. We can test L2TP by dialing in from the remote PC, first with the Rhelm-based user ID, and then with the User-based ID. We can test IP connectivity using PING from the PC client to the 2216.

We can monitor L2TP from ELS using `disp sub l2 all`. A sample talk 2 session from the 2216 LNS is shown in Figure 185.

```
Li *t 2
00:00:42   GW.001:

Copyright 1984 Massachusetts Institute of Technology,
Copyright 1989 The Regents of the University of California

00:12:12   L2.024: PAYLOAD SEND 38 bytes, net=10, callid=17957
00:12:12   L2.041: SND F=4902,L=50,Tid=58577,Cid=31030,NS=56,NR=54,O=0
00:12:12   L2.040: RCV F=4800,L=12,Tid=30892,Cid=17957,NS=54,NR=57,O=0
00:12:12   L2.043: RCV PAYLOAD Zero Len Body (ZLB), tid=30892,cid=17957
00:12:12   L2.040: RCV F=4900,L=50,Tid=30892,Cid=17957,NS=54,NR=57,O=0
00:12:12   L2.022: PAYLOAD RCVD 38 bytes, net 10, callid=17957
00:12:12   L2.023: Send PAYLOAD Zero Len Body (ZLB), tid=58577,cid=0
00:12:12   L2.041: SND F=4802,L=12,Tid=58577,Cid=31030,NS=57,NR=55,O=0
```

Figure 185. Monitoring L2TP from ELS

We can also check the L2TP tunnel state from talk 5 as shown in Figure 186.

```
Li Layer-2-Tunneling Console> tunnel state
Tunnel ID | Type | Peer ID |    State    | Time Since Chg | # Calls | Flags
    30892 | L2TP |   58577 | Established |     0: 4:31    |       1 |  TL  F

Li Layer-2-Tunneling Console>exit
```

Figure 186. Monitoring L2TP from Talk 5

9.6 Testing L2TP with IPSec Enabled

Now it is time to re-enable IPSec and verify that L2TP is still working.

After IPSec is re-enabled, we first check the IPSec tunnel's status with the `list all` command as shown in Figure 187.

```
Li +f ip
Li IPsec>list all

IPsec is ENABLED

Defined Manual Tunnels:

   ID         Name          Local IP Addr   Remote IP Addr   Mode    State
 ------  ---------------  ---------------  ---------------  -----  --------
      1  ESP&AH             192.168.189.1   192.168.189.59  TUNN   Enabled
      2  TRANS-ESP&AH       192.168.189.1   192.168.189.59  TRANS  Enabled

Tunnel Cache:

 ID     Local IP Addr   Remote IP Addr   Mode   Policy  Tunnel Expiration
-----  ---------------  ---------------  -----  ------  ------------------
    2    192.168.189.1   192.168.189.59  TRANS  ESP-AH  17:01  Jun 25 1998
    1    192.168.189.1   192.168.189.59  TUNN   ESP-AH  17:01  Jun 25 1998
Li IPsec>exit
Karen +
```

Figure 187. Verifying the IPSec Tunnels Are Enabled

We then verify that the L2TP tunnel is still working.

```
Li Layer-2-Tunneling Console> tunnel state
Tunnel ID | Type | Peer ID |    State    | Time Since Chg | # Calls | Flags
    30892 | L2TP |   58577 | Established |     0: 5:29    |       1 |  TL  F

Li Layer-2-Tunneling Console>exit
```

Figure 188. Monitoring L2TP with IPSec Enabled

To be sure that IPSec tunnel number 2 is being used for the L2TP traffic, we check the IPSec statistics and see if the send and receive counts are increasing. This is shown in Figure 189 on page 133.

```
Li IPsec>stats
Enter the Tunnel ID, Tunnel Name, or 'ALL' [ALL]? 2

                      Statistics For Secure Tunnel 2
Received:
  total pkts   AH packets   ESP packets   total bytes    AH bytes     ESP bytes
  ----------   ----------   -----------   -----------   ----------   ----------
      357842       178921        178921      36722368     20508236     16214132

Sent:
  total pkts   AH packets   ESP packets   total bytes    AH bytes     ESP bytes
  ----------   ----------   -----------   -----------   ----------   ----------
       80058        40029         40029       8401232      5001196      3400036

Receive Packet Errors:
   AH errors   AH bad seq   ESP errors   ESP bad seq
  ----------   ----------   ----------   -----------
           0            0            0             0

Send Packet Errors:
   AH errors   ESP errors
  ----------   ----------
           0            0
```

Figure 189. Checking the IPSec Statistics

We also check the IP packet filters to see how many times the filters were hit. This is shown in Figure 190 on page 134.

```
Li +p ip
Li IP>pac pf_out_0
Name              Dir  Intf  State  Src-Addr-Ver  #Access-Controls
pf_out_0          Out  0     On     N/A           4

Access Control currently enabled
Access Control facility: USER


Access Control run 808   times, 0 cache hits

List of access control records:

1   Type=I S   Source=192.168.180.0    Dest=192.168.157.0    Prot=  0-255
               Mask=  255.255.255.0    Mask=255.255.255.0    Use=4
               SPorts=N/A              DPorts=N/A            Tid=1
                                       Log=No

2   Type=I S   Source=9.24.105.0       Dest=192.168.157.0    Prot=  0-255
               Mask=  255.255.255.0    Mask=255.255.255.0    Use=0
               SPorts=N/A              DPorts=N/A            Tid=1
                                       Log=No

3   Type=I     Source=192.168.189.1    Dest=192.168.189.59   Prot= 50-51
               Mask=  255.255.255.255  Mask=255.255.255.255  Use=400
               SPorts=    0-65535      DPorts=    0-65535
                                       Log=No

4   Type=I S   Source=192.168.189.1    Dest=192.168.189.59   Prot=  0-255
               Mask=  255.255.255.255  Mask=255.255.255.255  Use=400
               SPorts=N/A              DPorts=N/A            Tid=2
                                       Log=No
```

Figure 190. Checking the Packet Filters

Note: Remember that in this case, the router is generating the traffic, so we need to look at access controls number 3 and 4. We see that they have been matched 400 times (Use=400).

This completes the configuration and testing of L2TP over an IPSec tunnel.

Appendix A. Basic Router Configuration

Before an IPSec tunnel can be defined, you need to have a valid IP configuration in the router. This consists of defining the hardware interfaces (2216) and adding IP interface addresses and submasks. There are several ways to accomplish this task.

- Config Only Mode (2216)
- EasyStart (2210)
- Explicit Talk 6 commands
- The Configuration Program
- Quick Config Process

In this appendix, we show you the Quick Config process that we used to build the network shown in Figure 38 on page 33. The *qconfig* process can be used to configure most of the functions of the router. Here, we just use it to define the physical interfaces and the IP addresses on these interfaces to get a valid IP configuration installed on the router.

For more information on configuring the 2210 or the 2216, please see *IBM 2210 Nways Multiprotocol Router Description and Configuration Scenarios Volume I*, SG24-4446 or *IBM 2216 Nways Multiaccess Connector Description and Configuration Scenarios Volume I*, SG24-4957, respectively.

A.1 Quick Config of the 2210 in the Branch Office

The sections below take you step-by-step through the qconfig command dialogs from the talk 6 command prompt on the 2210-24T that we used in our scenarios. Our purpose was to obtain a valid IP configuration so that it could be used as a base configuration for IPSec tunnel definitions. Figure 191 on page 136 through Figure 196 on page 141 show these configuration screens.

```
*t 6
Config>set hostname Karen
Host name updated successfully
Karen Config>qconfig

Router Quick Configuration for the following:
o   Interfaces
o   Multilink PPP (w/o DIALs)
o   Dial Circuits (w/o DIALs)
o   Dial-in Access to LANs (DIALs)
o   Bridging
        Spanning Tree Bridge (STB)
        Source Routing Bridge (SRB)
        Source Routing/Transparent Bridge (SR/TB)
        Source Routing Transparent Bridge (SRT)
o   Protocols
        IP (including OSPF, RIP and SNMP)
        IPX
        DNA (DECnet)
o   Booting
o   Service Port

Event Logging will be enabled for all configured subsystems
with logging level 'Standard'

Note:  Please be warned that any existing configuration for a particular item
will be removed if that item is configured through Quick Configuration
```

Figure 191. Quick Configuration (QCONFIG) for the 2210

```
*******************************************************
Interface Configuration
*******************************************************

Type 'Yes' to Configure Interfaces
Type 'No' to skip Interface Configuration
Type 'Quit' to exit Quick Config

Configure Interfaces? (Yes, No, Quit): [Yes]
Type 'r' any time at this level to restart Interface Configuration


Intf 0 is Token Ring
Speed in Mb/sec (4, 16): [16]
Connector (STP, UTP): [STP]

Intf 1 is WAN PPP
Encapsulation for WAN interface 1  (PPP, Frame Relay, V34): [PPP]
Cable type (RS-232 DTE, RS-232 DCE, V.35 DTE, V.35 DCE, V.36 DTE, X.21 DTE,
    X.21 DCE): [RS-232 DTE]

Intf 2 is WAN PPP
Encapsulation for WAN interface 2  (PPP, Frame Relay, V34): [PPP]
Cable type (RS-232 DTE, RS-232 DCE, V.35 DTE, V.35 DCE, V.36 DTE, X.21 DTE,
    X.21 DCE): [RS-232 DTE]

Intf 3 is WAN PPP
Encapsulation for WAN interface 3  (PPP, Frame Relay, V34): [PPP]
Cable type (RS-232 DTE, RS-232 DCE, V.35 DTE, V.35 DCE, V.36 DTE, X.21 DTE,
    X.21 DCE): [RS-232 DTE]

Intf 4 is WAN PPP
Encapsulation for WAN interface 4  (PPP, Frame Relay, V34): [PPP]
Cable type (RS-232 DTE, RS-232 DCE, V.35 DTE, V.35 DCE, V.36 DTE, X.21 DTE,
    X.21 DCE): [RS-232 DTE]

Intf 5 is Token Ring
Speed in Mb/sec (4, 16): [16]
Connector (STP, UTP): [STP]

ISDN Primary T1/J1 is not supported in this load.
Skipping this device.
```

Figure 192. Quick Configuration (QCONFIG) for the 2210

```
This is all configured device information:

Intf 0 is Token Ring, Speed 16 Mb/sec, Connector UTP
Intf 1 is WAN PPP, RS-232 DTE cable
Intf 2 is WAN PPP, RS-232 DTE cable
Intf 3 is WAN PPP, RS-232 DTE cable
Intf 4 is WAN PPP, RS-232 DTE cable
Intf 5 is Token Ring, Speed 16 Mb/sec, Connector UTP
Intf 6 is ISDN Primary T1/J1

Save this configuration? (Yes, No): [Yes]

Device  configuration saved

************************************************************
Multilink PPP Configuration (w/o DIALs)
************************************************************

Type 'Yes' to Configure Multilink PPP
Type 'No' to skip Multilink PPP Configuration
Type 'Quit' to exit Quick Config

Configure Multilink PPP? (Yes, No, Quit): [Yes] no

************************************************************
Dial Circuit Configuration (w/o DIALs)
************************************************************

Type 'Yes' to Configure Dial Circuits
Type 'No' to skip Dial Circuits Configuration
Type 'Quit' to exit Quick Config

Configure Dial Circuits? (Yes, No, Quit): [Yes] no

************************************************************
Dial-in Access to LANs (DIALs) Configuration
************************************************************

Type 'Yes' to Configure DIALs Configuration
Type 'No' to skip DIALs Configuration Configuration
Type 'Quit' to exit Quick Config

Configure DIALs Interfaces? (Yes, No, Quit): [Yes] no

Configure DIALs Server? (Yes, No, Quit): [Yes] no
```

Figure 193. Quick Configuration (QCONFIG) for the 2210

```
*********************************************************
Bridging Configuration
*********************************************************

Type ′Yes′ to Configure Bridging
Type ′No′ to skip Bridging Configuration
Type ′Quit′ to exit Quick Config

Configure Bridging? (Yes, No, Quit): [Yes] no

*********************************************************
Protocol Configuration
*********************************************************

Type ′Yes′ to Configure Protocols
Type ′No′ to skip Protocol Configuration
Type ′Quit′ to exit Quick Config

Configure Protocols? (Yes, No, Quit): [Yes]
Type ′r′ any time at this level to restart Protocol Configuration

Configure IP? (Yes, No): [Yes]
Type ′r′ any time at this level to restart IP Configuration

Configuring Per-Interface IP Information

Configuring Interface 0 (Token Ring)
Configure IP on this interface? (Yes, No): [Yes]
IP Address: [] 192.168.189.59
Address Mask: [255.255.255.0]

Configuring Interface 1 (WAN PPP)
Configure IP on this interface? (Yes, No): [Yes] no

Configuring Interface 2 (WAN PPP)
Configure IP on this interface? (Yes, No): [Yes] no

Configuring Interface 3 (WAN PPP)
Configure IP on this interface? (Yes, No): [Yes] no

Configuring Interface 4 (WAN PPP)
Configure IP on this interface? (Yes, No): [Yes] no

Configuring Interface 5 (Token Ring)
Configure IP on this interface? (Yes, No): [Yes]
IP Address: [] 192.168.157.59
Address Mask: [255.255.255.0]
```

Figure 194. Quick Configuration (QCONFIG) for the 2210

```
Configuring Interface 6 (ISDN Primary T1/J1)
IP cannot be configured directly on this interface

Per-Interface IP Configuration complete

Configuring IP Routing Information
Enable Dynamic Routing? (Yes, No): [Yes] no

Only Static Routing Enabled

Routing Configuration Complete

Configuring SNMP Information

SNMP will be configured with the following parameters:

     Community: public
     Access:    read_trap

If you plan to use the graphical configuration tool
to download a configuration, it requires the definition
of a community name with read_write_trap access.

Define community with read_write_trap access ? (Yes, No): [Yes] no

SNMP Configuration Complete

This is the information you have entered:

     Interface #     IP Address         Address Mask
          0          192.168.189.59     255.255.255.0
          5          192.168.157.59     255.255.255.0

Only STATIC Routing present.

SNMP has been configured with the following parameters:

     Community: public
     Access:    read_trap

If you plan to use the graphical configuration tool to
download a configuration, you will need to use the SNMP configuration
environment to define a community name with read_write_trap access.


Save this configuration? (Yes, No): [Yes]

IP configuration saved
```

Figure 195. Quick Configuration (QCONFIG) for the 2210

```
Configure IPX? (Yes, No): [Yes] no

Configure DNA? (Yes, No): [Yes] no

************************************************************
Booting Configuration
************************************************************

Type 'Yes' to Configure Booting
Type 'No' to skip Booting Configuration
Type 'Quit' to exit Quick Config

Configure Booting? (Yes, No, Quit): [Yes] no

************************************************************
Service Port Configuration
************************************************************

Type 'Yes' to Configure Service Ports
Type 'No' to skip Service Ports Configuration
Type 'Quit' to exit Quick Config

Configure service port? (Yes, No, Quit): [Yes] no

Quick Config Done
Restart the router for this configuration to take effect.

Restart the router? (Yes, No): [Yes]

RESTARTING THE ROUTER........
```

Figure 196. Quick Configuration (QCONFIG) for the 2210

This completes the Quick Config of the 2210 in the branch office.

A.2 Quick Config of the 2216 In the Data Center

On a 2210, in the case of the LAN and WAN ports, the hardware interfaces are a fixed configuration and no additional steps are required to add interfaces.

Note: You do have to add interfaces in the case of dial circuits.

On the 2216, you need to first add the devices to the configuration before they can be configured.

A.2.1 Adding the Interfaces

Before we run the Quick Config process on the 2216, we must first configure the interfaces. In Figure 197 on page 142, we show you how we added the devices for our scenarios. These include two token-ring interfaces, two Ethernet interfaces, a V35/V36 PPP interface and a V35/V36 frame relay interface. These are added via the add device command from the talk 6 prompt.

The order of adding the interfaces is arbitrary. However, the network numbers for your interfaces will be different depending upon the order that you added them to the configuration.

Note: Your 2216 will probably have a different hardware configuration with different adapters in different slots. Look carefully at which devices are in which slots of your 2216.

```
*t 6
Config>set hostname Li
Host name updated successfully
Li Config>add dev token-ring
Device Slot #(1-8) [1]?
Device Port #(1-2) [1]?
Adding Token Ring device in slot 1  port 1 as interface #0
Use "net 0" to configure Token Ring parameters
Li Config>add dev token-ring
Device Slot #(1-8) [1]?
Device Port #(1-2) [2]?
Adding Token Ring device in slot 1  port 2 as interface #1
Use "net 1" to configure Token Ring parameters
Li Config>add dev ethernet
Device Slot #(1-8) [1]? 5
Device Port #(1-2) [1]?
Adding Ethernet device in slot 5  port 1 as interface #2
Use "net 2" to configure Ethernet parameters
Li Config>add dev ethernet
Device Slot #(1-8) [1]? 5
Device Port #(1-2) [2]?
Adding Ethernet device in slot 5  port 2 as interface #3
Use "net 3" to configure Ethernet parameters
Li Config>add dev V35/V36
Device Slot #(1-8) [1]? 6
Device Port #(0-5) [0]?
Defaulting Data-link protocol to PPP
Adding V.35/V.36 PPP device in slot 6  port 0 as interface #4
Use "set data-link" command to change the data-link protocol
Use "net 4" to configure V.35/V.36 PPP parameters
Li Config>add dev V35/V36
Device Slot #(1-8) [1]? 6
Device Port #(0-5) [0]? 1
Defaulting Data-link protocol to PPP
Adding V.35/V.36 PPP device in slot 6  port 1 as interface #5
Use "set data-link" command to change the data-link protocol
Use "net 5" to configure V.35/V.36 PPP parameters
Li Config>set data-link frame-relay
Interface Number [0]? 5
Li Config>list dev
Ifc 0     Token Ring                      Slot: 1   Port: 1
Ifc 1     Token Ring                      Slot: 1   Port: 2
Ifc 2     Ethernet                        Slot: 5   Port: 1
Ifc 3     Ethernet                        Slot: 5   Port: 2
Ifc 4     V.35/V.36 PPP                   Slot: 6   Port: 0
Ifc 5     V.35/V.36 Frame Relay           Slot: 6   Port: 1
Li Config>
```

Figure 197. Adding Devices to the 2216

For more information on adding devices to a 2216 configuration, please see *IBM 2216 Nways Multiaccess Connector Description and Configuration Scenarios Volume I*, SG24-4957.

After we add the hardware interfaces, we need to configure the parameters for these interfaces. We use the net <ifc#> command to configure these parameters. For our scenarios, we set the ring speed of the token-ring

interfaces to 16 Mbps and the media type to shielded twisted pair. For the Ethernet interfaces, we set the connector type to RJ45 (10BASET).

```
Li Config>net 0
Token-Ring interface configuration
Li TKR config>speed 16
Li TKR config>media shielded
Li TKR config>exit
Li Config>net 1
Token-Ring interface configuration
Li TKR config>speed 16
Li TKR config>media shielded
Li TKR config>exit
Li Config>net 2
Ethernet interface configuration
Li ETH config>connector-type rj45
Li ETH config>exit
Li Config>net 3
Ethernet interface configuration
Li ETH config>connector-type rj45
Li ETH config>exit
Li Config>
```

Figure 198. Setting Interface Parameters on the 2216

Now, we are ready to do the IP protocol configuration of the 2216. In this example, we use the *qconfig* command although we could also use direct configuration commands from the IP configuration sub-menu of talk 6.

```
Li Config>qconfig

Router Quick Configuration for the following:
o   Bridging
        Spanning Tree Bridge (STB)
        Source Routing Bridge (SRB)
        Source Routing/Transparent Bridge (SR/TB)
o   Protocols
        IP (including OSPF, RIP and SNMP)
        IPX
        DNA (DECnet)

Event Logging will be enabled for all configured subsystems
with logging level 'Standard'

Note:  Please be warned that any existing configuration for a particular item
will be removed if that item is configured through Quick Configuration

**********************************************************
Bridging Configuration
**********************************************************

Type 'Yes' to Configure Bridging
Type 'No' to skip Bridging Configuration
Type 'Quit' to exit Quick Config

Configure Bridging? (Yes, No, Quit): [Yes] no
```

Figure 199. Quick Configuration (QCONFIG) for the 2216

```
*******************************************************
Protocol Configuration
*******************************************************

Type 'Yes' to Configure Protocols
Type 'No' to skip Protocol Configuration
Type 'Quit' to exit Quick Config

Configure Protocols? (Yes, No, Quit): [Yes]
Type 'r' any time at this level to restart Protocol Configuration

Configure IP? (Yes, No): [Yes]
Type 'r' any time at this level to restart IP Configuration

Configuring Per-Interface IP Information

Configuring Interface 0 (Token Ring)
Configure IP on this interface? (Yes, No): [Yes]
IP Address: [] 192.168.189.1
Address Mask: [255.255.255.0]

Configuring Interface 1 (Token Ring)
Configure IP on this interface? (Yes, No): [Yes]
IP Address: [] 192.168.188.1
Address Mask: [255.255.255.0]

Configuring Interface 2 (Ethernet)
Configure IP on this interface? (Yes, No): [Yes]
IP Address: [] 9.24.105.172
Address Mask: [255.0.0.0] 255.255.255.0

Configuring Interface 3 (Ethernet)
Configure IP on this interface? (Yes, No): [Yes]
IP Address: [] 192.168.180.1
Address Mask: [255.255.255.0]

Configuring Interface 4 (V.35/V.36 PPP)
Configure IP on this interface? (Yes, No): [Yes] no

Configuring Interface 5 (V.35/V.36 Frame Relay)
Configure IP on this interface? (Yes, No): [Yes] no

Per-Interface IP Configuration complete

Configuring IP Routing Information
Enable Dynamic Routing? (Yes, No): [Yes] no

Only Static Routing Enabled

Routing Configuration Complete
```

Figure 200. Quick Configuration (QCONFIG) for the 2216

```
Configuring SNMP Information

SNMP will be configured with the following parameters:

     Community: public
     Access:    read_trap

If you plan to use the graphical configuration tool
to download a configuration, it requires the definition
of a community name with read_write_trap access.

Define community with read_write_trap access ? (Yes, No): [Yes] no

SNMP Configuration Complete

This is the information you have entered:

     Interface #     IP Address         Address Mask
          0          192.168.189.1      255.255.255.0
          1          192.168.188.1      255.255.255.0
          2          9.24.105.172       255.255.255.0
          3          192.168.180.1      255.255.255.0

Only STATIC Routing present.

SNMP has been configured with the following parameters:

     Community: public
     Access:    read_trap

If you plan to use the graphical configuration tool to
download a configuration, you will need to use the SNMP configuration
environment to define a community name with read_write_trap access.


Save this configuration? (Yes, No): [Yes]

IP configuration saved
```

Figure 201. Quick Configuration (QCONFIG) for the 2216

```
Configure IPX? (Yes, No): [Yes] no

Configure DNA? (Yes, No): [Yes] no

Quick Config Done
Do you want to write this configuration? (Yes, No): [Yes]
Config Save: Using bank A and config number 1

Configuration was written.
The system must be restarted for this configuration to take effect.
Li Config> <CTRL>+<P>
Li *reload
Are you sure you want to reload the gateway? (Yes or [No]): yes
The configuration has been changed, save it? (Yes or ·No‘ or Abort): yes
Config Save: Using bank A and config number 1
The configuration has been saved.
```

Figure 202. Quick Configuration (QCONFIG) for the 2216

This completes the Quick Config of the 2216 in the data center.

Appendix B. Configuring the IPSec Tunnels at the Data Center

This appendix provides the screens that we used in configuring the IPSec tunnels and the packet filters for the IBM 2216 Nways Multiaccess Connector in the data center for the scenario described in Chapter 3, “Connecting the Data Center to the Branch Office” on page 33.

We start by creating the packet filters as shown in Figure 203.

```
Li *t 6
Gateway user configuration
Li Config>protocol ip
Internet protocol user configuration
Li IP config>add packet-filter
Packet-filter name []? pf_out_0
Filter incoming or outgoing traffic? [IN]? out
Which interface is this filter for [0]?
Li IP config>add packet-filter
Packet-filter name []? pf_in_0
Filter incoming or outgoing traffic? [IN]?
Which interface is this filter for [0]?
Li IP config>
```

Figure 203. Creating Packet Filters on the Public Interface (0)

Then we update the outbound packet filter. We first add an access control for communication between the two intranet LANs at the corporate site and the intranet LAN at the branch office via tunnel 1. See Figure 204 for these commands.

```
Li IP config>update packet-filter pf_out_0
Li Packet-filter 'pf_out_0' Config>add access-control
Enter type [E]? s
Internet source [0.0.0.0]? 192.168.180.0
Source mask [255.255.255.255]? 255.255.255.0
Internet destination [0.0.0.0]? 192.168.157.0
Destination mask [255.255.255.255]? 255.255.255.0
Enter starting protocol number ([0] for all protocols) [0]?
Enter IPsec Tunnel ID [1]?
Enable Logging(Yes or [No]):
Li Packet-filter 'pf_out_0' Config>add access-control
Enter type [E]? s
Internet source [0.0.0.0]? 9.24.105.0
Source mask [255.255.255.255]? 255.255.255.0
Internet destination [0.0.0.0]? 192.168.157.0
Destination mask [255.255.255.255]? 255.255.255.0
Enter starting protocol number ([0] for all protocols) [0]?
Enter IPsec Tunnel ID [1]?
Enable Logging(Yes or [No]):
Li Packet-filter 'pf_out_0' Config>
```

Figure 204. Configuring the Outbound Packet Filter

Next we add an access control for the IPSec packets that are sent by router Li to router Karen. See Figure 205 on page 150 for the command.

```
Li Packet-filter 'pf_out_0' Config>add access-control
Enter type [E]? i
Internet source [0.0.0.0]? 192.168.189.1
Source mask [255.255.255.255]?
Internet destination [0.0.0.0]? 192.168.189.59
Destination mask [255.255.255.255]?
Enter starting protocol number ([0] for all protocols) [0]? 50
Enter ending protocol number [50]? 51
Enable Logging(Yes or [No]):
Li Packet-filter 'pf_out_0' Config>
```

Figure 205. Configuring the Outbound Packet Filter

Finally, we add the access control for all non-IPSec traffic between the two routers. This traffic is sent via tunnel 2. See Figure 206 for the command.

```
Li Packet-filter 'pf_out_0' Config>add access-control
Enter type [E]? s
Internet source [0.0.0.0]? 192.168.189.1
Source mask [255.255.255.255]?
Internet destination [0.0.0.0]? 192.168.189.59
Destination mask [255.255.255.255]?
Enter starting protocol number ([0] for all protocols) [0]?
Enter IPsec Tunnel ID [1]? 2
Enable Logging(Yes or [No]):
Li Packet-filter 'pf_out_0' Config>
```

Figure 206. Configuring the Outbound Packet Filter

Next we list the access controls in the outbound packet filter.

```
Li Packet-filter 'pf_out_0' Config>list access-control
Access Control is: disabled
Access Control facility: USER

List of access control records:

1   Type=I S   Source=192.168.180.0    Dest=192.168.157.0    Prot=  0-255
               Mask=  255.255.255.0    Mask=255.255.255.0
               SPorts=N/A              DPorts=N/A            Tid=1
                                       Log=No

2   Type=I S   Source=9.24.105.0       Dest=192.168.157.0    Prot=  0-255
               Mask=  255.255.255.0    Mask=255.255.255.0
               SPorts=N/A              DPorts=N/A            Tid=1
                                       Log=No

3   Type=I     Source=192.168.189.1    Dest=192.168.189.59   Prot= 50-51
               Mask=  255.255.255.255  Mask=255.255.255.255
               SPorts=    0-65535      DPorts=    0-65535
                                       Log=No

4   Type=I S   Source=192.168.189.1    Dest=192.168.189.59   Prot=  0-255
               Mask=  255.255.255.255  Mask=255.255.255.255
               SPorts=N/A              DPorts=N/A            Tid=2
                                       Log=No
Li Packet-filter 'pf_out_0' Config>exit
Li IP config>
```

Figure 207. Listing Access Controls

Then we add access controls to the inbound packet filter. We start with the access control for IPsec packets coming in from router Karen.

```
Li IP config>update packet-filter pf_in_0
Li Packet-filter 'pf_in_0' Config>add access-control
Enter type [E]? i
Internet source [0.0.0.0]? 192.168.189.59
Source mask [255.255.255.255]?
Internet destination [0.0.0.0]? 192.168.189.1
Destination mask [255.255.255.255]?
Enter starting protocol number ([0] for all protocols) [0]? 50
Enter ending protocol number [50]? 51
Enable Logging(Yes or [No]):
Li Packet-filter 'pf_in_0' Config>
```

Figure 208. Configuring the Inbound Packet Filter

Then we add the access control for communication between the intranet LANs via tunnel 1.

```
Li Packet-filter 'pf_in_0' Config>add access-control
Enter type [E]? s
Internet source [0.0.0.0]? 192.168.157.0
Source mask [255.255.255.255]? 255.255.255.0
Internet destination [0.0.0.0]? 192.168.180.0
Destination mask [255.255.255.255]? 255.255.255.0
Enter starting protocol number ([0] for all protocols) [0]?
Enter IPsec Tunnel ID [1]?
Enable Logging(Yes or [No]):
Li Packet-filter 'pf_in_0' Config>add access-control
Enter type [E]? s
Internet source [0.0.0.0]? 192.168.157.0
Source mask [255.255.255.255]? 255.255.255.0
Internet destination [0.0.0.0]? 9.24.105.0
Destination mask [255.255.255.255]? 255.255.255.0
Enter starting protocol number ([0] for all protocols) [0]?
Enter IPsec Tunnel ID [1]?
Enable Logging(Yes or [No]):
Li Packet-filter 'pf_in_0' Config>
```

Figure 209. Configuring the Inbound Packet Filter

Finally, we add the access control for router-to-router traffic via tunnel 2.

```
Li Packet-filter 'pf_in_0' Config>add access-control
Enter type [E]? s
Internet source [0.0.0.0]? 192.168.189.59
Source mask [255.255.255.255]?
Internet destination [0.0.0.0]? 192.168.189.1
Destination mask [255.255.255.255]?
Enter starting protocol number ([0] for all protocols) [0]?
Enter IPsec Tunnel ID [1]? 2
Enable Logging(Yes or [No]):
Li Packet-filter 'pf_in_0' Config>
```

Figure 210. Configuring the Inbound Packet Filter

Here is the list of access controls in the inbound packet filter.

```
Li Packet-filter 'pf_in_0' Config>list access-control
Access Control is: disabled
Access Control facility: USER

List of access control records:

1   Type=I     Source=192.168.189.59   Dest=192.168.189.1    Prot= 50-51
               Mask=  255.255.255.255  Mask=255.255.255.255
               SPorts=    0-65535      DPorts=    0-65535
                                       Log=No

2   Type=I S   Source=192.168.157.0    Dest=192.168.180.0    Prot=  0-255
               Mask=  255.255.255.0    Mask=255.255.255.0
               SPorts=N/A              DPorts=N/A            Tid=1
                                       Log=No

3   Type=I S   Source=192.168.157.0    Dest=9.24.105.0       Prot=  0-255
               Mask=  255.255.255.0    Mask=255.255.255.0
               SPorts=N/A              DPorts=N/A            Tid=1
                                       Log=No

4   Type=I S   Source=192.168.189.59   Dest=192.168.189.1    Prot=  0-255
               Mask=  255.255.255.255  Mask=255.255.255.255
               SPorts=N/A              DPorts=N/A            Tid=2
                                       Log=No
Li Packet-filter 'pf_in_0' Config>exit
Li IP config>
```

Figure 211. Listing the Access Controls

Next we enable the packet filters and set access control on. The listing of the packet filters shows that access control is on and that the state of the packet filters is on.

```
Li IP config>enable packet-filter
Enter packet-filter name to be enabled []? pf_in_0
Li IP config>enable packet-filter
Enter packet-filter name to be enabled []? pf_out_0
Li IP config>set access-control on
Li IP config>list packet-filter

List of packet-filter records:

Name              Direction   Interface   State  Src-Addr-Ver
pf_in_0           In          0           On     Off
pf_out_0          Out         0           On     N/A
Access Control is: enabled
Li IP config>exit
```

Figure 212. Enabling Access Control

Next we go into the IPSec feature configuration to add tunnel 1.

```
Li Config>feature ipsec
IP Security feature user configuration
Li IPsec config>add tunnel
Tunnel ID (1-65535) [1]?
Tunnel Name (optional) []? ESP&AH1
Tunnel Lifetime, in minutes (0-525600) [46080]?
Tunnel Encapsulation Mode (TUNN or TRANS) [TUNN]?
Tunnel Policy (AH,ESP,AH-ESP,ESP-AH) [AH-ESP]?
```

Figure 213. Defining the Tunnel-Mode IPSec Tunnel

Next, we are prompted to define the local end of the SA. Figure 214 shows the required parameters.

```
Local IP Address [192.168.189.1]?
Local Authentication SPI (256-65535) [256]?
Local Authentication Algorithm (HMAC-MD5,HMAC-SHA) [HMAC-MD5]?
Local Authentication Key (32 characters) in Hex (0-9,a-f,A-F):
Enter Local Authentication Key again (32 characters) in Hex (0-9,a-f,A-F):
Local Encryption SPI (256-65535) [256]?
Local Encryption Algorithm (DES-CBC,CDMF,3DES) [DES-CBC]?
Local Encryption Key (16 characters) in Hex (0-9,a-f,A-F):
Enter Local Encryption Key again (16 characters) in Hex (0-9,a-f,A-F):
Additional Padding for Local Encryption (0-120) [0]?
Do you wish to use local ESP authentication? [No]:
```

Figure 214. Defining the Tunnel-Mode IPSec Tunnel

Note that the keys are not displayed while typed.

Next, we are prompted to define the remote end of the SA. Figure 215 shows the required parameters.

```
Remote IP Address [0.0.0.0]? 192.168.189.59
Remote Authentication SPI (1-65535) [256]?
Remote Authentication Algorithm (HMAC-MD5,HMAC-SHA) [HMAC-MD5]?
Remote Authentication Key (32 characters) in Hex (0-9,a-f,A-F):
Enter Remote Authentication Key again (32 characters) in Hex (0-9,a-f,A-F):
Remote Encryption SPI (1-65535) [256]?
Remote Encryption Algorithm (DES-CBC,CDMF,3DES) [DES-CBC]?
Remote Encryption Key (16 characters) in Hex (0-9,a-f,A-F):
Enter Remote Encryption Key again (16 characters) in Hex (0-9,a-f,A-F):
Do you wish to perform verification of remote encryption padding? [No]:
Do you wish to use remote ESP authentication? [No]:
Enable replay prevention? [No]:
Do you wish to enable this tunnel? [Yes]:
Li IPsec config>
```

Figure 215. Defining the Tunnel-Mode IPSec Tunnel

The next tunnel we create is the transport-mode tunnel with id=2 and we have chosen to use AH-ESP again as the tunnel policy, the value of 257 for all SPIs, AH protocol using HMAC-MD5 and 3DES encryption algorithm.

Figure 216 shows the configuration of the transport-mode tunnel.

```
Li IPsec config>add tunnel
Tunnel ID (1-65535) [1]? 2
Tunnel Name (optional) []? TRANS-ESP&AH
Tunnel Lifetime, in minutes (0-525600) [46080]?
Tunnel Encapsulation Mode (TUNN or TRANS) [TUNN]? TRANS
Tunnel Policy (AH,ESP,AH-ESP,ESP-AH) [AH-ESP]?
```

Figure 216. Defining the Transport-Mode IPSec Tunnel

Next, we are prompted to define the local end of the SA. Figure 217 shows the required parameters.

```
Local IP Address [192.168.189.1]?
Local Authentication SPI (256-65535) [256]? 257
Local Authentication Algorithm (HMAC-MD5,HMAC-SHA) [HMAC-MD5]?
Local Authentication Key (32 characters) in Hex (0-9,a-f,A-F):
Enter Local Authentication Key again (32 characters) in Hex (0-9,a-f,A-F):
Local Encryption SPI (256-65535) [257]?
Local Encryption Algorithm (DES-CBC,CDMF,3DES) [DES-CBC]? 3DES
First Local Encryption Key (16 characters) in Hex (0-9,a-f,A-F):
Enter First Local Encryption Key again (16 characters) in Hex (0-9,a-f,A-F):
Second Local Encryption Key (16 characters) in Hex (0-9,a-f,A-F):
Enter Second Local Encryption Key again (16 characters) in Hex (0-9,a-f,A-F):
Third Local Encryption Key (16 characters) in Hex (0-9,a-f,A-F):
Enter Third Local Encryption Key again (16 characters) in Hex (0-9,a-f,A-F):
Additional Padding for Local Encryption (0-120) [0]?
Do you wish to use local ESP authentication? [No]:
```

Figure 217. Defining the Transport-Mode IPSec Tunnel

Next, we are prompted to define the remote end of the SA. Figure 218 on page 156 shows the required parameters.

```
Remote IP Address [0.0.0.0]? 192.168.189.59
Remote Authentication SPI (1-65535) [257]?
Remote Authentication Algorithm (HMAC-MD5,HMAC-SHA) [HMAC-MD5]?
Remote Authentication Key (32 characters) in Hex (0-9,a-f,A-F):
Enter Remote Authentication Key again (32 characters) in Hex (0-9,a-f,A-F):
Remote Encryption SPI (1-65535) [257]?
Remote Encryption Algorithm (DES-CBC,CDMF,3DES) [3DES]?
First Remote Encryption Key (16 characters) in Hex (0-9,a-f,A-F):
Enter First Remote Encryption Key again (16 characters) in Hex (0-9,a-f,A-F):
Second Remote Encryption Key (16 characters) in Hex (0-9,a-f,A-F):
Enter Second Remote Encryption Key again (16 characters) in Hex (0-9,a-f,A-F):
Third Remote Encryption Key (16 characters) in Hex (0-9,a-f,A-F):
Enter Third Remote Encryption Key again (16 characters) in Hex (0-9,a-f,A-F):
Do you wish to perform verification of remote encryption padding? [No]:
Do you wish to use remote ESP authentication? [No]:
Enable replay prevention? [No]:
Do you wish to enable this tunnel? [Yes]:
Li IPsec config>
```

Figure 218. Defining the Transport-Mode IPSec Tunnel

Next, we list the tunnels that we have created. Figure 219 shows the command and output.

```
Li IPsec config>list tunnel all

   ID         Name          Local IP Addr   Remote IP Addr   Mode    State
 ------  ---------------  ---------------  ---------------  -----  --------
      2  TRANS-ESP&AH     192.168.189.1    192.168.189.59   TRANS  Enabled
      1  ESP&AH1          192.168.189.1    192.168.189.59   TUNN   Enabled
Li IPsec config>
```

Figure 219. Listing Defined Tunnels

The last step is to enable IPSec on the router. Figure 220 shows this command.

```
Li IPsec config>enable ipsec
Restarting the router is required for IPSec to be active.
Li IPsec config>exit
Li Config>
```

Figure 220. Enabling IPSec

Next, we have to reload the 2216 so that the newly created IPSec tunnel will be activated.

```
Li Config> <CTRL>+<P>
Li *reload
Are you sure you want to reload the gateway? (Yes or [No]): yes
The configuration has been changed, save it? (Yes or [No] or Abort): yes
Config Save: Using bank A and config number 2
The configuration has been saved.
```

Figure 221. Reloading the Router

This completes the configuration of the IPSec tunnels and the packet filters for the data center router.

Appendix C. Special Notices

This publication is intended to help networking professionals quickly understand the functions of Nways Multiprotocol Access Services and Nways Multiprotocol Routing Services. The information in this publication is not intended as the specification of any programming interfaces that are provided by Nways Multiprotocol Access Services or Nways Multiprotocol Routing Services. See the PUBLICATIONS section of the IBM Programming Announcement for Nways Multiprotocol Access Services and Nways Multiprotocol Routing Services for more information about what publications are considered to be product documentation.

References in this publication to IBM products, programs or services do not imply that IBM intends to make these available in all countries in which IBM operates. Any reference to an IBM product, program, or service is not intended to state or imply that only IBM′s product, program, or service may be used. Any functionally equivalent program that does not infringe any of IBM′s intellectual property rights may be used instead of the IBM product, program or service.

Information in this book was developed in conjunction with use of the equipment specified, and is limited in application to those specific hardware and software products and levels.

IBM may have patents or pending patent applications covering subject matter in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to the IBM Director of Licensing, IBM Corporation, North Castle Drive, Armonk, NY 10504-1785.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact IBM Corporation, Dept. 600A, Mail Drop 1329, Somers, NY 10589 USA.

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The information contained in this document has not been submitted to any formal IBM test and is distributed AS IS. The information about non-IBM (″vendor″) products in this manual has been supplied by the vendor and IBM assumes no responsibility for its accuracy or completeness. The use of this information or the implementation of any of these techniques is a customer responsibility and depends on the customer′s ability to evaluate and integrate them into the customer′s operational environment. While each item may have been reviewed by IBM for accuracy in a specific situation, there is no guarantee that the same or similar results will be obtained elsewhere. Customers attempting to adapt these techniques to their own environments do so at their own risk.

Any pointers in this publication to external Web sites are provided for convenience only and do not in any manner serve as an endorsement of these Web sites.

Any performance data contained in this document was determined in a controlled environment, and therefore, the results that may be obtained in other operating environments may vary significantly. Users of this document should verify the applicable data for their specific environment.

The following document contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples contain the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

Reference to PTF numbers that have not been released through the normal distribution process does not imply general availability. The purpose of including these reference numbers is to alert IBM customers to specific information relative to the implementation of the PTF when it becomes available to each customer according to the normal IBM PTF distribution process.

The following terms are trademarks of the International Business Machines Corporation in the United States and/or other countries:

Advanced Peer-to-Peer Networking	APPN
eNetwork	ESCON
IBM	Nways
OS/2	OS/390
S/370	S/390
VTAM	

The following terms are trademarks of other companies:

C-bus is a trademark of Corollary, Inc.

Java and HotJava are trademarks of Sun Microsystems, Incorporated.

Microsoft, Windows, Windows NT, and the Windows 95 logo are trademarks or registered trademarks of Microsoft Corporation.

PC Direct is a trademark of Ziff Communications Company and is used by IBM Corporation under license.

Pentium, MMX, ProShare, LANDesk, and ActionMedia are trademarks or registered trademarks of Intel Corporation in the U.S. and other countries.

UNIX is a registered trademark in the United States and other countries licensed exclusively through X/Open Company Limited.

Other company, product, and service names may be trademarks or service marks of others.

Appendix D. Related Publications

The publications listed in this section are considered particularly suitable for a more detailed discussion of the topics covered in this redbook.

D.1 International Technical Support Organization Publications

For information on ordering these ITSO publications see “How to Get ITSO Redbooks” on page 163.

- *A Comprehensive Guide to Virtual Private Networks, Volume I: IBM Firewall, Server and Client Solutions,* SG24-5201
- *IBM 2216 Nways Multiaccess Connector Description and Configuration Scenarios - Volume I*, SG24-4957
- *IBM 2210 Nways Multiprotocol Router Description and Configuration Scenarios - Volume I*, SG24-4446
- *IBM 2210 Nways Multiprotocol Router IBM 2216 Nways Multiaccess Connector Description and Configuration Scenarios - Volume II*, SG24-4956
- *IBM 2216 Multiaccess Connector ESCON Solutions*, SG24-2137
- *Inside APPN - The Essential Guide to the Next-Generation SNA*, SG24-3669
- *TCP/IP Tutorial and Technical Overview*, GG24-3376

D.2 Redbooks on CD-ROMs

Redbooks are also available on CD-ROMs. **Order a subscription** and receive updates 2-4 times a year at significant savings.

CD-ROM Title	Subscription Number	Collection Kit Number
System/390 Redbooks Collection	SBOF-7201	SK2T-2177
Networking and Systems Management Redbooks Collection	SBOF-7370	SK2T-6022
Transaction Processing and Data Management Redbook	SBOF-7240	SK2T-8038
Lotus Redbooks Collection	SBOF-6899	SK2T-8039
Tivoli Redbooks Collection	SBOF-6898	SK2T-8044
AS/400 Redbooks Collection	SBOF-7270	SK2T-2849
RS/6000 Redbooks Collection (HTML, BkMgr)	SBOF-7230	SK2T-8040
RS/6000 Redbooks Collection (PostScript)	SBOF-7205	SK2T-8041
RS/6000 Redbooks Collection (PDF Format)	SBOF-8700	SK2T-8043
Application Development Redbooks Collection	SBOF-7290	SK2T-8037

D.3 Other Publications

These publications are also relevant as further information sources:

- *Nways Multiprotocol Routing Services Software User's Guide*, SC30-3681
- *Nways Multiprotocol Routing Services Protocol Configuration and Monitoring Reference, Volume 1*, SC30-3680
- *Nways Multiprotocol Routing Services Protocol Configuration and Monitoring Reference, Volume 2*, SC30-3865
- *Nways Multiprotocol Access Services Software User's Guide*, SC30-3886

- *Nways Multiprotocol Access Services Protocol Configuration and Monitoring Reference, Volume 1*, SC30-3884
- *Nways Multiprotocol Access Services Protocol Configuration and Monitoring Reference, Volume 2*, SC30-3885
- *Nways Event Logging System Messages Guide*, SC30-3682
- *Configuration Program User's Guide for Nways Multiprotocol Access Services and Multiprotocol Routing Services*, GC30-3830
- *SNA APPN Architecture Reference*, SC30-3422
- *VTAM Network Implementation Guide V4R4 for MVS/ESA*, SC31-8370
- *VTAM Resource Definition Reference V4R4 for MVS/ESA*, SC31-8377
- *Applied Cryptography*, second edition, John Wiley & Sons, Inc., 1996, by Bruce Schneier; ISBN 0-471-11709-9.
- *Network Security: Private Communication in a Public World*, PTR Prentice Hall, 1995, by Charlie Kaufman, Radia Perlman, and Mike Speciner; ISBN 0-13-061466-1.

How to Get ITSO Redbooks

This section explains how both customers and IBM employees can find out about ITSO redbooks, redpieces, and CD-ROMs. A form for ordering books and CD-ROMs by fax or e-mail is also provided.

- **Redbooks Web Site** http://www.redbooks.ibm.com/

  Search for, view, download or order hardcopy/CD-ROMs redbooks from the redbooks Web site. Also read redpieces and download additional materials (code samples or diskette/CD-ROM images) from this redbooks site.

  Redpieces are redbooks in progress; not all redbooks become redpieces and sometimes just a few chapters will be published this way. The intent is to get the information out much quicker than the formal publishing process allows.

- **E-mail Orders**

  Send orders via e-mail including information from the redbook order form to:

	IBMMAIL	**Internet**
In United States:	usib6fpl at ibmmail	usib6fpl@ibmmail.com
In Canada:	caibmbkz at ibmmail	lmannix@vnet.ibm.com
Outside North America:	dkibmbsh at ibmmail	bookshop@dk.ibm.com

- **Telephone Orders**

United States (toll free)	1-800-879-2755	
Canada (toll free)	1-800-IBM-4YOU	
Outside North America	(long distance charges apply)	
(+45) 4810-1320 - Danish	(+45) 4810-1220 - French	(+45) 4810-1270 - Norwegian
(+45) 4810-1420 - Dutch	(+45) 4810-1020 - German	(+45) 4810-1120 - Spanish
(+45) 4810-1540 - English	(+45) 4810-1620 - Italian	(+45) 4810-1170 - Swedish
(+45) 4810-1670 - Finnish		

This information was current at the time of publication, but is continually subject to change. The latest information for customers may be found at http://www.redbooks.ibm.com/ and for IBM employees at http://w3.itso.ibm.com/.

IBM Intranet for Employees

IBM employees may register for information on workshops, residencies, and redbooks by accessing the IBM Intranet Web site at http://w3.itso.ibm.com/ and clicking the ITSO Mailing List button. Look in the Materials repository for workshops, presentations, papers, and Web pages developed and written by the ITSO technical professionals; click the Additional Materials button. Employees may also view redbook, residency and workshop announcements at http://inews.ibm.com/.

IBM Redbook Fax Order Form

Fax your redbook orders to:

United States (toll free)	1-800-445-9269
Canada	1-403-267-4455
Outside North America	(+45) 48 14 2207 (long distance charge)

Please send me the following:

Title	Order Number	Quantity

First name Last name

Company

Address

City Postal code Country

Telephone number Telefax number VAT number

- Invoice to customer number
- Credit card number

Credit card expiration date Card issued to Signature

We accept American Express, Diners, Eurocard, Master Card, and Visa. Payment by credit card not available in all countries. Signature mandatory for credit card payment.

Index

Numerics

A

B

C

D

E

F

M

N

O

P

R

S

T

U

V

W

ITSO Redbook Evaluation

A Comprehensive Guide to Virtual Private Networks, Volume II:
SG24-5234-00

Your feedback is very important to help us maintain the quality of ITSO redbooks. **Please complete this questionnaire and fax it to: USA International Access Code + 1 914 432 8264 or:**

- Use the online evaluation form found at http://www.redbooks.ibm.com
- Send your comments in an Internet note to redbook@us.ibm.com

Which of the following best describes you?
__Customer __Business Partner __Solution Developer __IBM employee
__None of the above

Please rate your overall satisfaction with this book using the scale:
(1 = very good, 2 = good, 3 = average, 4 = poor, 5 = very poor)

Overall Satisfaction _____

Please answer the following questions:

Was this redbook published in time for your needs? Yes____ No____

If no, please explain:

_____

_____

_____

_____

What other redbooks would you like to see published?

_____

_____

_____

Comments/Suggestions: **(THANK YOU FOR YOUR FEEDBACK!)**

_____

_____

_____

_____

_____

SG24-5234-00
Printed in the U.S.A.