May 2004
LR1102A-T1/E1
LR1104A-T1/E1
LR1112A-T1/E1
LR1114A-T1/E1

Black Box LR11xx Series Router Configurations

CUSTOMER SUPPORT INFORMATION

Order **toll-free** in the U.S. 24 hours, 7 A.M. Monday to midnight Friday: **877-877-BBOX**
FREE technical support, 24 hours a day, 7 days a week: Call **724-746-5500** or fax **724-746-0746**
Mail order: **Black Box Corporation**, 1000 Park Drive, Lawrence, PA 15055-1018
Web site: **www.blackbox.com** • E-mail: **info@blackbox.com**

FEDERAL COMMUNICATIONS COMMISSION

AND

CANADIAN DEPARTMENT OF COMMUNICATIONS

RADIO FREQUENCY INTERFERENCE STATEMENTS

This equipment generates, uses, and can radiate radio frequency energy and if not installed and used properly, that is, in strict accordance with the manufacturer's instructions, may cause interference to radio communication. It has been tested and found to comply with the limits for a Class A computing device in accordance with the specifications in Subpart B of Part 15 of FCC rules, which are designed to provide reasonable protection against such interference when the equipment is operated in a commercial environment. Operation of this equipment in a residential area is likely to cause interference, in which case the user at his own expense will be required to take whatever measures may be necessary to correct the interference.

Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

This digital apparatus does not exceed the Class A limits for radio noise emission from digital apparatus set out in the Radio Interference Regulation of the Canadian Department of Communications.

Le présent appareil numérique n'émet pas de bruits radioélectriques dépassant les limites applicables aux appareils numériques de la classe A prescrites dans le Règlement sur le brouillage radioélectrique publié par le ministère des Communications du Canada.

Normas Oficiales Mexicanas (NOM)

Electrical Safety Statement

INSTRUCCIONES DE SEGURIDAD

1. Todas las instrucciones de seguridad y operación deberán ser leídas antes de que el aparato eléctrico sea operado.

2. Las instrucciones de seguridad y operación deberán ser guardadas para referencia futura.

3. Todas las advertencias en el aparato eléctrico y en sus instrucciones de operación deben ser respetadas.

4. Todas las instrucciones de operación y uso deben ser seguidas.

5. El aparato eléctrico no deberá ser usado cerca del agua—por ejemplo, cerca de la tina de baño, lavabo, sótano mojado o cerca de una alberca, etc.

6. El aparato eléctrico debe ser usado únicamente con carritos o pedestales que sean recomendados por el fabricante.

7. El aparato eléctrico debe ser montado a la pared o al techo sólo como sea recomendado por el fabricante.

8. Servicio—El usuario no debe intentar dar servicio al equipo eléctrico más allá a lo descrito en las instrucciones de operación. Todo otro servicio deberá ser referido a personal de servicio calificado.

9. El aparato eléctrico debe ser situado de tal manera que su posición no interfiera su uso. La colocación del aparato eléctrico sobre una cama, sofá, alfombra o superficie similar puede bloquea la ventilación, no se debe colocar en libreros o gabinetes que impidan el flujo de aire por los orificios de ventilación.

10. El equipo eléctrico deber ser situado fuera del alcance de fuentes de calor como radiadores, registros de calor, estufas u otros aparatos (incluyendo amplificadores) que producen calor.

11. El aparato eléctrico deberá ser connectado a una fuente de poder sólo del tipo descrito en el instructivo de operación, o como se indique en el aparato.

12. Precaución debe ser tomada de tal manera que la tierra fisica y la polarización del equipo no sea eliminada.

13. Los cables de la fuente de poder deben ser guiados de tal manera que no sean pisados ni pellizcados por objetos colocados sobre o contra ellos, poniendo particular atención a los contactos y receptáculos donde salen del aparato.

14. El equipo eléctrico debe ser limpiado únicamente de acuerdo a las recomendaciones del fabricante.

15. En caso de existir, una antena externa deberá ser localizada lejos de las lineas de energia.

16. El cable de corriente deberá ser desconectado del cuando el equipo no sea usado por un largo periodo de tiempo.

17. Cuidado debe ser tomado de tal manera que objectos liquidos no sean derramados sobre la cubierta u orificios de ventilación.

18. Servicio por personal calificado deberá ser provisto cuando:

A: El cable de poder o el contacto ha sido dañado; o

B: Objectos han caído o líquido ha sido derramado dentro del aparato; o

C: El aparato ha sido expuesto a la lluvia; o

D: El aparato parece no operar normalmente o muestra un cambio en su desempeño; o

E: El aparato ha sido tirado o su cubierta ha sido dañada.

Contents

1
DHCP RELAY

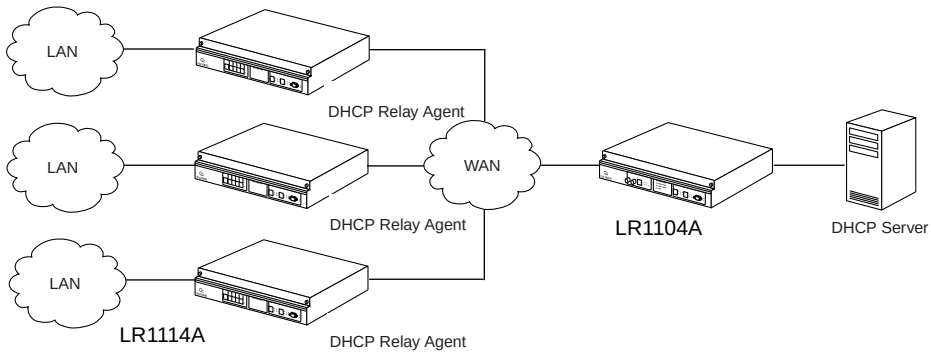
1.1DHCP Relay

This application describes the functionality of the DHCP relay feature and includes CLI command examples.

1.1.1 Feature Overview

Black Box DHCP relay feature eliminates the need for a DHCP server on every LAN, because DHCP requests can be relayed to a single remote DHCP server. Black Box's implementation of DHCP relay is based on RFC 1532. BOOTP/DHCP messages are relayed (vs. forwarded) between the server and client.

Figure 1 DHCP Relay Overview



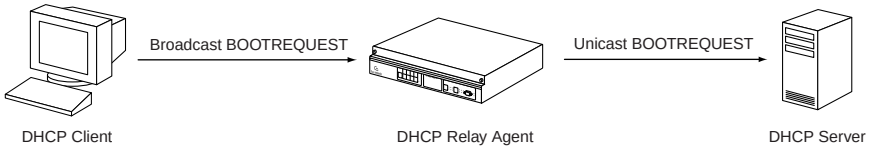
1.1.2 Functionality

The DHCP relay feature uses BOOTP requests and replies to negotiate packet delivery between the DHCP client and server.

1.1.2.1 BOOTP Requests

BOOTP requests are messages from client to server. Request messages include DHCP DISCOVER, DHCP REQUEST, DHCP RELEASE, etc. The relay agent modifies the packet header by adding relay information to the DHCP gateway address (giaddr) field. The server replies to the gateway address specified in the packet's giaddr field.

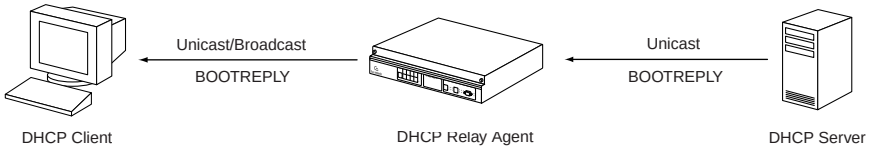
Figure 2 BOOTP Requests



1.1.2.2 BOOTP Replies

BOOTP replies are messages from the server to the client. Reply messages include DHCP OFFER, DHCP ACK, DHCP NAK, etc. The relay agent looks up the MAC address and either sends the packet to the client or broadcasts it on the LAN.

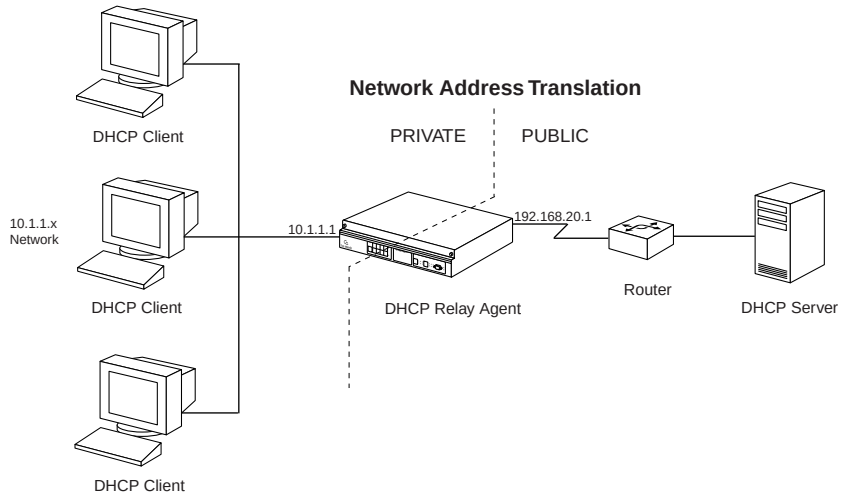
Figure 3 BOOTP Replies



1.1.3 Using DHCP Relay with NAT

When NAT is enabled, the DHCP server may discard packets because the giaddr does not match the source of the packet. Additionally, it may not know how to route the packet back to the client. See Figure 4. The solution is that the gateway address (giaddr) field needs to have IP address 192.168.20.1 (in this example). The DHCP server configuration should be able to give 10.1.1.x addresses for packets from 192.168.20.1. However, there may be a limitation that the DHCP server does not allow configuration using IP addresses from a different subnet, although this is mentioned in the RFC.

Figure 4 A Typical Scenario



1.1.4 Command Line Interface

The following are examples of command strings relevant to DHCP relay:

1.1.4.1 Enabling DHCP Relay

```
Blackbox> configure terminal
Blackbox/configure> interface ethernet 0
Blackbox/configure/interface/ethernet 0> dhcp server_address 20.1.1.1
```

1.1.4.2 Disabling DHCP Relay

```
Blackbox/configure/interface/ethernet 0> no dhcp server_address 20.1.1.1
```

1.1.4.3 Configuring the Gateway Address field when NAT is enabled

```
Blackbox/configure/interface/ethernet 0> dhcp gateway_address 192.168.20.1
```

1.1.5 Displaying DHCP Configuration

The following screen captures show the displayed results of issuing show commands relevant to DHCP relay, with and without gateway addresses configured.

Figure 5 show dhcp_relay Command

```
> show dhcp_relay

DHCP RELAY CONFIGURATION
---------------------------
Ethernet 0: Disabled
Ethernet 1: Enabled: DHCP Server 10.1.1.1
```

Figure 6 show dhcp_relay Command

```
> show dhcp_relay

DHCP RELAY CONFIGURATION
---------------------------
Ethernet 0: Disabled
Ethernet 1: Enabled: DHCP Server 10.1.1.1 (Gateway
Address: 192.168.20.1)
```

1.1.6 Displaying Statistics

Figure 7 Displaying Ethernet Interface Statistics

```
> show interface ethernet 1


ethernet 1
ipaddr       192.168.120.1
netmask      255.255.255.0
description  -
status       down, operationally down
configured   auto
  speed       -
  mode        -
actual
  speed      100
  mode       half_duplex
mtu          1500

ethernet1 (unit number 1)
Type: ETHERNET (802.3)
Flags: (0x807c203)  UP, MULTICAST-ROUTE
Internet Address: 192.168.120.1
Internet Netmask: 255.255.255.0
Internet Broadcast: 192.168.120.255
Maximum Transfer Unit: 1500 bytes
Mac Address:  00:00:23:00:60:01

port counters since last boot/clear
  Bytes Rx                          0  Bytes Tx                          0

  Packets Rx                        0  Packets Tx                        0

  Runts Rx                          0  Collisions                        0

  Babbels Rx                        0  Late Collisions                   0

  Err Packets Rx                    0  Up/Down States (Phys)             0

  Up/Down States (Admin)              2

port counters for the last five minutes
  Bytes Rx                          0  Bytes Tx                          0

  Packets Rx                        0  Packets Tx                        0

  Runts Rx                          0  Collisions                        0

  Babbels Rx                        0  Late Collisions                   0
```

1.1.7 DHCP Limitations

There are limitations when using DHCP relay on a Black Box system. Only one DHCP server can be specified per interface. DHCP can be enabled only on Ethernet interfaces (not on bundles). And last, DHCP can be enabled in IP routing (static and dynamic) mode, but not in IP Mux mode.

2
CONFIGURING INTERNET GROUP MANAGEMENT PROTOCOL

2.1IGMP Configuration

Internet Group Management Protocol (IGMP) is enabled on hosts and routers that want to receive multicast traffic. IGMP informs locally-attached routers of their multicast group memberships. Hosts inform routers of the groups of which they are members by multicasting IGMP Group Membership Reports. When multicast routers listen for these reports, they can exchange group membership information with other multicast routers. This reporting system allows distribution trees to be formed to deliver multicast datagrams. The original version of IGMP was defined in RFC 1112, Host Extensions for IP Multicasting. Extensions to IGMP, known as IGMP version 2.

IGMPv2 improves performance and supports the following message types:

- IGMP Query: IGMP Query is sent by the router to know which groups have members on the attached network.
- IGMP Reports: IGMP reports are sent as a response to the query by hosts to announce their group membership. Reports can be sent “unsolicited” when the hosts come up.
- IGMP Leaves: IGMP Leaves are sent by the host when it relinquishes membership of a group.

The latest extension to the IGMP standard is Version 3, which includes interoperability with version 2 and version 1 hosts, also provides support for source filtering. Source filtering enables a multicast receiver host to signal to a router which groups it wants to receive multicast traffic from, and from which source(s) this traffic is expected. This membership information enables the router to forward traffic only from those sources from which receivers requested the traffic.

IGMPv3 supports applications that explicitly signal sources from which they want to receive traffic. With IGMPv3, receivers signal membership to a multicast host group in the following two modes:

- INCLUDE mode: In this mode, the receiver announces membership to a host group and provides a list of IP addresses (the INCLUDE list) from which it wants to receive traffic.
- EXCLUDE mode: In this mode, the receiver announces membership to a host group and provides a list of IP addresses (the EXCLUDE list) from which it does not want to receive traffic. This indicates that the host wants to receive traffic only from other sources whose IP addresses are not listed in the EXCLUDE list. To receive traffic from all sources, like in the case of the Internet Standard Multicast (ISM) service model, a host expresses EXCLUDE mode membership with an empty EXCLUDE list.

IGMPv3 is used by the hosts to express their desire to be a part of the source-specific multicast (SSM) which is an emerging standard used by routers to direct multicast traffic to the host only if its is from a specific source.

2.1.1 IGMP Commands

The IGMP commands are:

ip igmp
ignore-v1-messages
ignore-v2-messages
last-member-query-count
last-member-query-interval
query-interval
query-response-interval
require-router-alert
robustness
send-router-alert
startup-query-count
startup-query-interval
group filter
version
debug ip igmp
debug ip igmp state
debug ip igmp normal
debug ip igmp packet query
debug ip igmp packet report
debug ip igmp packet leave
show ip igmp groups
show ip igmp interface
clear ip igmp groups

2.1.2 IGMP Configuration Examples

Use the examples shown in this section to use IGMP in multicast configurations.

2.1.2.1 Example 1

The following example enables IGMP.

```
Blackbox/configure> ip igmp
```

2.1.2.2 Example 2

With the command line still in Interface Configuration Mode, the following example disables IGMP.

```
Blackbox/configure> no ip igmp
```

2.1.2.3 Example 3

In the following example, the **ignore-v1-messages** command is used to disable processing of IGMPv1 messages on interface ethernet 0.

```
Blackbox/configure/ip/igmp/interface ethernet0> ignore-v1-messages
Blackbox/configure/ip/igmp/interface ethernet0> exit 3
Blackbox/configure>
```

2.1.2.4 Example 4

In the following example, the **ignore-v2-messages** command disables processing of IGMPv1 messages on interface ethernet 0.

```
Blackbox/configure/ip/igmp/interface ethernet0> ip igmp ignore-v2-messages
Blackbox/configure/ip/igmp/interface ethernet0> exit 3
Blackbox/configure>
```

2.1.2.5 Example 5

The following example configures the Last Member Query Count to be 4 on ethernet 0.

```
Blackbox/configure/ip/igmp/interface ethernet0> last-member-query-count 4
```

2.1.2.6 Example 6

In the following example for interface ethernet 0, the Robustness is configured to be 4. The Last Member Query count is configured to be 5.

```
Blackbox/configure/ip/igmp/interface ethernet0> robustness 4
Blackbox/configure/ip/igmp/interface ethernet0> last-member-query-count 5
Blackbox/configure/ip/igmp/interface ethernet0> exit 3
Blackbox/configure>
```

2.1.2.7 Example 7

The following example configures ethernet 0 with the default Last Member Query Interval of 2000 milliseconds (20 seconds).

```
Blackbox/configure/ip/igmp/interface ethernet0> last-member-query-interval 2000
```

2.1.2.8 Example 8

The following example configures ethernet 0 with the default Query Interval to be 200 seconds.

```
Blackbox/configure/ip/igmp/interface ethernet0> query-interval 200
```

2.1.2.9 Example 9

The following example configures the default Query Response Interval to be 10 seconds (or 100 deciseconds) for ethernet 0.

```
Blackbox/configure/ip/igmp/interface ethernet0> query-response-time 100
```

2.1.2.10Example 10

The following example turns require-router-alert on for interface ethernet 0.

```
Blackbox/configure/ip/igmp/interface ethernet0> require-router-alert
```

2.1.2.11Example 11

The following example configures the default Robustness to be 3 for interface ethernet 0.

```
Blackbox/configure/ip/igmp/interface ethernet0> ip igmp robustness 3
```

2.1.2.12Example 12

The following example turns the send-router-alert option off for interface ethernet 1.

```
Blackbox/configure/ip/igmp/interface ethernet1> no send-router-alert
```

2.1.2.13Example 13

The following example configures IGMP version 2 to run on interface ethernet 0.

```
Blackbox/configure/ip/igmp/interface ethernet0> version 2
Blackbox/configure/ip/igmp/interface ethernet0> exit 3
Blackbox/configure>
```

3w
FILTERING IP TRAFFIC

3.1IP Packet Filter Lists

Black Box systems can be configured for IP traffic filtering capabilities. IP traffic filtering allows creation of rule sets that selectively block TCP/IP packets on a specified interface. Filters are applied independently to all interfaces: Ethernet, serial, or WAN, as well as independently to interface direction: IN (packets coming in to the Black Box system) or OUT (packets going out of the Black Box system).

IP packet filtering capability can be used to restrict access to the Black Box system from untrusted, external networks or from specific, internal networks. An example would be a filter that prohibits external users from establishing Telnet sessions to the Black Box system, and allows only specific internal users Telnet access to the system.

- At the end of every rule list is an implied “deny all traffic” statement. Therefore, all packets not explicitly permitted by filtering rules, are denied. This effectively means that once you enter a “deny” statement in your filter list, you are implicitly denying all packets from crossing the interface. Therefore, it is important that each filter list contain at least one “permit” statement.
- The order in which you enter the filtering rules is important. As the Black Box system is evaluating each packet, the Black Box OS tests the packet against each rule statement sequentially. After a match is found, no more rule statements are checked. For example, if you create a rule statement that explicitly permits all traffic, all traffic is passed since no further rules are checked.
- The Black Box OS permits easy re-ordering of filter commands through **filter_list insert** and **delete** commands.

3.1.1 Example1

Consider a Black Box connected via a bundle “WAN1” (wan IP address 200.1.1.1) to an ISP, with Ethernet 0 (IP address 222.199.19.3) connected to the internal network. The network administrator wants to completely block Telnet access to the Black Box from all external networks as well as from all internal networks except 222.199.19.0/28. All other TCP/IP traffic, such as FTP, Ping, and HTTP, is to flow unrestricted through the Black Box system.

3.1.1.1 Configure the Black Box LR1104A.

```
Blackbox> configure term
Blackbox/configure> ip
Blackbox/configure/ip> filter_list filtera   (gives the list a name)
Blackbox/configure/ip/filter_list> add deny tcp any 200.1.1.1 dport =23
Blackbox/configure/ip/filter_list> add permit tcp 222.199.19.0/28 222.199.19.3 dport =23
Blackbox/configure/ip/filter_list> add deny tcp any 222.199.19.3 dport =23
Blackbox/configure/ip/filter_list> add permit ip any any
Blackbox/configure/ip/filter_list> exit
```

```
Blackbox/configure/ip> apply_filter ether0 filtera in
Blackbox/configure/ip> apply_filter WAN1 filtera in
Blackbox/configure/ip> exit
Blackbox/configure> exit
Blackbox> save local
```

3.1.2 Example 2

Consider the same network addressing as in example 1. The network administrator has a slightly different requirement - he wishes to permit FTP sessions from all networks to the internal FTP server (222.199.19.12), deny FTP sessions to all other addresses, and permit all other traffic to flow through the Black Box unit.

3.1.2.1 Configure the Black Box LR1104A

```
Blackbox> configure terminal
Blackbox/configure> ip
Blackbox/configure/ip> filter_list filterb   (gives the list a name)
Blackbox/configure/ip/filter_list> add permit tcp any 222.199.19.12 dport =21
Blackbox/configure/ip/filter_list> add deny tcp any 222.199.19.0 dport =21
Blackbox/configure/ip/filter_list> add permit ip any any
Blackbox/configure/ip/filter_list> exit

Blackbox/configure/ip> apply_filter WAN1 filterb in
Blackbox/configure/ip> exit
Blackbox/configure> exit
Blackbox> save local
```

3.1.3 Example 3

Example 3 focuses on a filter list where the network administrator is specifically denying all traffic from a specific external network (197.100.200.0/24) access through the Black Box unit.

3.1.3.1 Configure the Black Box LR1104A

```
Blackbox> configure terminal
Blackbox/configure> ip
Blackbox/configure/ip> filter_list filterc   (gives the list a name)
Blackbox/configure/ip/filter_list> add deny ip 197.100.200.0/24 any
Blackbox/configure/ip/filter_list> add permit ip any any
Blackbox/configure/ip/filter_list> exit

Blackbox/configure/ip> apply_filter WAN1 filterc in
Blackbox/configure/ip> exit
Blackbox/configure> exit
Blackbox> save local
```

4
CONFIGURING SECURITY

4.1IPSec Configurations

This guide provides information and examples on how to configure IPSec.

There are three licenses that control access to the features:

- Basic VPN Management (`vpn_mgmt`)—allows users to manage a remote Black Box router.
- Firewall (`firewall`)—allows users to manage the firewall features. Also includes Basic VPN Management.
- Advanced VPN and firewall (`vpn_plus_firewall`)—Allows users to manage remote LANs. Also includes Basic VPN and Firewall licenses.

To see the licenses available in this release, enter:

```
Blackbox/configure> system licenses ?

NAME
  licenses - Configure feature upgrade licenses

SYNTAX
  licenses license_type <cr>

DESCRIPTION
  license_type        -- Specifies the type of feature upgrade license
    The parameter may have any of the following values:
        enable_1_port -- Enable  1 port
        enable_2_ports-- Enable  2 ports
        enable_3_ports-- Enable  3 ports
        enable_4_ports-- Enable  4 ports
        BGP4          -- BGP4 routing
        vpn_mgmt      -- Enable VPN Mgmt License
        firewall      -- Enable Firewall and VPN Mgmt License
        vpn_plus_firewall-- Enable Advance VPN and Firewall License
```

To install the advanced VPN and firewall license and use all the security features available in this release, enter:

```
Blackbox/configure> system licenses vpn_plus_firewall
Enter Security Upgrade License key: 024f3bc296b4ea7265
```

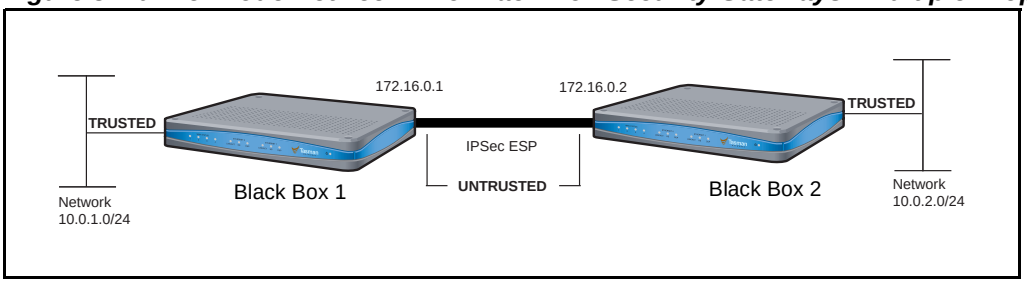
4.2 Example 1: Managing the Black Box LR1104A Securely Over an IPSec Tunnel

The following example demonstrates how to manage a Black Box router through an IP security tunnel. Steps are presented for configuring the Black Box1 and Black Box2 routers to assist any host on the LAN side of Black Box-2 to manage the Black Box1 router through the IP security tunnel.

The security requirements are as follows:

- Phase 1: 3DES with SHA1
- Phase 2: IPSec ESP with AES and HMAC-SHA1

Figure 8 Tunnel Mode Between Two Black Box Security Gateways - Multiple Proposals



Step 1: Configure a WAN bundle of network type untrusted

```
Black Box1/configure> interface bundle wan1
  message: Configuring new bundle
Black Box1/configure/interface/bundle wan1> link t1 1
Black Box1/configure/interface/bundle wan1> encapsulation ppp
Black Box1/configure/interface/bundle wan1> ip address 172.16.0.1 24
Black Box1/configure/interface/bundle wan1> crypto untrusted
Black Box1/configure/interface/bundle wan1> exit
```

Step 2: Configure the Ethernet interface with trusted network type

```
Black Box1/configure> interface ethernet 0
  message: Configuring existing Ethernet interface
Black Box1/configure interface/ethernet 0> ip address 10.0.1.1 24
Black Box1/configure/interface/ethernet 0> crypto trusted
Black Box1/configure/interface/ethernet 0> exit
```

Step 3: Display the crypto interfaces

```
Blackbox> show crypto interfaces

Interface      Network
Name           Type
---------      -------
wan1           Untrusted
ethernet0      trusted

Blackbox>
```

Step 4: Add route to peer LAN

```
Black Box1/configure> ip route 10.0.2.0 24 wan1
```

Step 5: Configure IKE to the peer gateway

```
Black Box1/configure> crypto ike policy Black Box2 172.16.0.2
Black Box1/configure/crypto/ike/policy Black Box2 172.16.0.2> local-address 172.16.0.1
  message: Default proposal created with priority1-des-sha1-pre_shared-g1.
  message: Key String has to be configured by the user.
Black Box1/configure/crypto/ike/policy Black Box2 172.16.0.2> key secretkey
Black Box1/configure/crypto/ike/policy Black Box2 172.16.0.2> proposal 1
Black Box1/configure/crypto/ike/policy Black Box2 172.16.0.2/proposal 1> encryption-algorithm
3des-cbc
Black Box1/configure/crypto/ike/policy Black Box2 172.16.0.2/proposal 1> exit
Black Box1/configure/crypto/ike/policy Black Box2 172.16.0.2> exit
```

Step 6: Display IKE policies

```
Blackbox> show crypto ike policy all

Policy     Peer            Mode       Transform
------     ----            ----       ---------
Black Box 172.14.0.2     Main        P1 pre-g1-3des-sha

Blackbox>
```

Step 7: Display IKE policies in detail

Displays the encryption algorithm, hash algorithm, authentication mode, and other details of the IKE policies.

Step 8: Configure the IPSec tunnel to the remote host

```
Black Box1/configure/crypto> ipsec policy Black Box2 172.16.0.2
Black Box1/configure/crypto/ipsec/policy Black Box2 172.16.0.2> match address 172.16.0.1 32
10.0.2.0 24
  message: Default proposal created with priority1-esp-3des-sha1-tunnel and activated.
Black Box1/configure/crypto/ipsec/policy Black Box2 172.16.0.2> proposal 1
Black Box1/configure/crypto/ipsec/policy Black Box2 172.16.0.2/proposal 1>
encryption-algorithm aes128-cbc
Black Box1/configure/crypto/ipsec/policy Black Box2 172.16.0.2/proposal 1> exit
Black Box1/configure/crypto/ipsec/policy Black Box2 172.16.0.2> exit
```

Step 9: Display IPSec policies

Displays the policy just added.

Step 10: Display IPSec policies in detail

Shows the details of the IPSec policies.

Step 10.1: Configure firewall policies to allow IKE negotiation through untrusted interface (applicable only if firewall license is also enabled)

```
Black Box1/configure> firewall internet
Black Box1/configure/firewall internet> policy 1000 in service ike self
Black Box1/configure/firewall internet/policy 1000 in> exit
Black Box1/configure/firewall internet> exit
```

Step 10.2: Configure firewall policies to allow desired services through untrusted interface to manage the router (applicable only if firewall license is also enabled)

```
Black Box1/configure> firewall internet
Black Box1/configure/firewall internet> policy 1001 in service snmp self
Black Box1/configure/firewall internet/policy 1001 in> exit
Black Box1/configure/firewall internet> policy 1002 in service telnet self
Black Box1/configure/firewall internet/policy 1002 in> exit
Black Box1/configure/firewall internet> policy 1003 in protocol icmp self
Black Box1/configure/firewall internet/policy 1003 in> exit
Black Box1/configure/firewall internet> exit
```

Step 10.3: Display firewall policies in the internet map (applicable only if firewall license is enabled)

```
Black Box1> show firewall policy internet
Advanced: S - Self Traffic, F - Ftp-Filter, H - Http-Filter,
          R - Rpc-Filter, N - Nat-Ip/Nat-Pool, L - Logging,
          E - Policy Enabled, M - Smtp-Filter

Pri  Dir Source Addr        Destination Addr   Sport Dport Proto Action Advanced
---  --- -----------        ----------------   ----------------- ------ --------
1000 in  any                any                ike               PERMIT SE
1001 in  any                any                snmp              PERMIT SE
1002 in  any                any                telnet            PERMIT SE
1003 in  any                any                any   any   icmp  PERMIT SE
1024 out any                any                any   any   any   PERMIT SE
```

Step 10.4: Display firewall policies in the internet map in detail (applicable only if firewall license is enabled)

```
Black Box1> show firewall policy internet detail

Policy with Priority 1000 is enabled, Direction is inbound
Action permit, Traffic is self
Logging is disable
Source Address is any, Dest Address is any
Source Port is any, Service Name is ike
Schedule is disabled, Ftp-Filter is disabled
Smtp-Filter is disabled, Http-Filter is disabled
Rpc-Filter is disabled, Nat is disabled
Bytes In 0, Bytes Out 0

Policy with Priority 1001 is enabled, Direction is inbound
Action permit, Traffic is self
Logging is disable
Source Address is any, Dest Address is any
Source Port is any, Service Name is snmp
Schedule is disabled, Ftp-Filter is disabled
Smtp-Filter is disabled, Http-Filter is disabled
Rpc-Filter is disabled, Nat is disabled
Bytes In 0, Bytes Out 0

Policy with Priority 1002 is enabled, Direction is inbound
Action permit, Traffic is self
Logging is disable
Source Address is any, Dest Address is any
Source Port is any, Service Name is telnet
Schedule is disabled, Ftp-Filter is disabled
Smtp-Filter is disabled, Http-Filter is disabled
Rpc-Filter is disabled, Nat is disabled
Bytes In 0, Bytes Out 0

Policy with Priority 1003 is enabled, Direction is inbound
Action permit, Traffic is self
Logging is disable
Source Address is any, Dest Address is any
Source Port is any, Dest Port is any, Protocol is icmp
Schedule is disabled, Ftp-Filter is disabled
Smtp-Filter is disabled, Http-Filter is disabled
Rpc-Filter is disabled, Nat is disabled
Bytes In 0, Bytes Out 0
Policy with Priority 1024 is enabled, Direction is outbound
Action permit, Traffic is self
Logging is disable
Source Address is any, Dest Address is any
Source Port is any, Dest Port is any, any
Schedule is disabled, Ftp-Filter is disabled
Smtp-Filter is disabled, Http-Filter is disabled
Rpc-Filter is disabled, Nat is disabled
Bytes In 0, Bytes Out 0
```

Step 11: Enable SNMP on the Black Box1 router

```
Black Box1/configure/crypto/> exit
Black Box1/configure> snmp
Black Box1/configure/snmp> community public rw
Black Box1/configure/snmp> exit
```

Step 12: Display SNMP communities

```
Blackbox>show snmp communities

Community = public, privileges=rw

Blackbox>
```

Step 13: Repeat steps 1 - 10 with suitable modifications on Black Box2 prior to managing Black Box1 from Black Box2's LAN side

Step 14: Test the IPSec tunnel for managing the Black Box1 router from a host on Black Box2's LAN.

Step 15: When the SNMP manager starts managing Black Box1 from Black Box2's LAN, display the IKE and IPSec SA tables using:

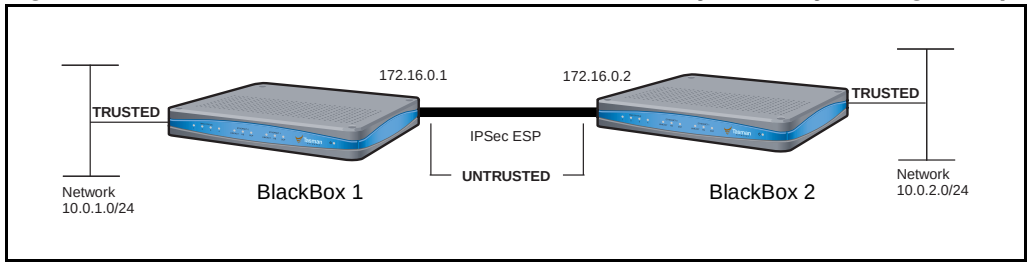
```
show crypto ike sa all
show crypto ike sa all detail
show crypto ipsec sa all
show crypto ipsec sa all detail
```

4.3 Example 2: Single Proposal: Tunnel Mode Between Two Black Box Security Gateways

The following example demonstrates how to form an IP security tunnel to join two private networks: 10.0.1.0/24 and 10.0.2.0/24. The security requirements are as follows:

- Phase 1: 3DES with SHA1
- Phase 2: IPSec ESP with AES (256-bit) and HMAC-SHA1

Figure 9 Tunnel Mode Between Two Black Box Security Gateways - Single Proposals



Step 1: Configure a WAN bundle of network type untrusted

```
Black Box1/configure/interface/bundle wan1> link t1 1
Black Box1/configure/interface/bundle wan1> encapsulation ppp
Black Box1/configure/interface/bundle wan1> ip address 172.16.0.1 24
Black Box1/configure/interface/bundle wan1> crypto untrusted
Black Box1/configure/interface/bundle wan1> exit
```

Step 2: Configure the Ethernet interface with trusted network type

```
Black Box1/configure> interface ethernet 0
  message: Configuring existing Ethernet interface
Black Box1/configure interface/ethernet 0> ip address 10.0.1.1 24
Black Box1/configure/interface/ethernet 0> crypto trusted
Black Box1/configure/interface/ethernet 0> exit
```

Step 3: Display the crypto interfaces

```
Blackbox> show crypto interfaces

Interface      Network
Name           Type
---------      -------
wan1           Untrusted
ethernet0      trusted

Blackbox>
```

Step 4: Add route to peer LAN

```
Black Box1/configure> ip route 10.0.2.0 24 wan1
```

Step 5: Configure IKE to the peer gateway

```
Black Box1/configure> crypto ike policy Black Box2 172.16.0.2
Black Box1/configure/crypto/ike/policy Black Box2 172.16.0.2> local-address 172.16.0.1
  message: Default proposal created with priority1-des-sha1-pre_shared-g1.
  message: Key String has to be configured by the user.
Black Box1/configure/crypto/ike/policy Black Box2 172.16.0.2> key secretkey
Black Box1/configure/crypto/ike/policy Black Box2 172.16.0.2> proposal 1
Black Box1/configure/crypto/ike/policy Black Box2 172.16.0.2/proposal 1> encryption-algorithm
3des-cbc
Black Box1/configure/crypto/ike/policy Black Box2 172.16.0.2> proposal 1> exit
Black Box1/configure/crypto/ike/policy Black Box2 172.16.0.2> exit
Black Box1/configure/crypto/exit
Black Box1/configure>
```

Step 6: Display IKE policies

```
Blackbox> show crypto ike policy all

Policy     Peer            Mode       Transform
------     ----            ----       ---------
Black Box 172.14.0.2     Main        P1 pre-g1-3des-sha

Blackbox>
```

Step 7: Configure IPSec tunnel to the remote host

```
Black Box1/configure/crypto> ipsec policy Black Box2 172.16.0.2
Black Box1/configure/crypto/ipsec/policy Black Box2 172.16.0.2> match address 10.0.1.0 24
10.0.2.0 24
```

NOTE

For IPSec only – when you create an outbound tunnel, an inbound tunnel is automatically created. The inbound tunnel applies the name that you provide for the outbound tunnel and adds the prefix “IN” to the name.

```
  message: Default proposal created with priority1-esp-3des-sha1-tunnel and activated.
Black Box1/configure/crypto/ipsec/policy Black Box2 172.16.0.2> proposal 1
Black Box1/configure/crypto/ipsec/policy Black Box2 172.16.0.2/proposal 1>
encryption-algorithm aes256-cbc
Black Box1/configure/crypto/ipsec/policy Black Box2 172.16.0.2/proposal 1> exit
Black Box1/configure/crypto/ipsec/policy Black Box2 172.16.0.2> exit
```

Step 8: Display IPSec policies

Using the `show crypto ipsec policy all` command.

Step 8.1: Configure firewall policies to allow IKE negotiation through untrusted interface (applicable only if firewall license is also enabled)

```
Black Box1/configure> firewall internet
Black Box1/configure/firewall internet> policy 1000 in service ike self
Black Box1/configure/firewall internet/policy 1000 in> exit
Black Box1/configure/firewall internet> exit
```

Step 8.2: Display firewall policies in the internet map (applicable only if firewall license is enabled)

```
Black Box1> show firewall policy internet
Advanced: S - Self Traffic, F - Ftp-Filter, H - Http-Filter,
          R - Rpc-Filter, N - Nat-Ip/Nat-Pool, L - Logging,
          E - Policy Enabled, M - Smtp-Filter

Pri  Dir Source Addr        Destination Addr   Sport Dport Proto Action Advanced
---  --- -----------        ----------------   ----------------- ------ --------
1000 in  any                any                ike               PERMIT SE
1024 out any                any                any   any   any   PERMIT SE
```

Step 8.3: Display firewall policies in the internet map in detail (applicable only if firewall license is enabled)

```
Black Box1> show firewall policy internet detail

Policy with Priority 1000 is enabled, Direction is inbound
Action permit, Traffic is self
Logging is disable
Source Address is any, Dest Address is any
Source Port is any, Service Name is ike
Schedule is disabled, Ftp-Filter is disabled
Smtp-Filter is disabled, Http-Filter is disabled
Rpc-Filter is disabled, Nat is disabled
Bytes In 0, Bytes Out 0

Policy with Priority 1024 is enabled, Direction is outbound
Action permit, Traffic is self
Logging is disable
Source Address is any, Dest Address is any
Source Port is any, Dest Port is any, any
Schedule is disabled, Ftp-Filter is disabled
Smtp-Filter is disabled, Http-Filter is disabled
Rpc-Filter is disabled, Nat is disabled
Bytes In 0, Bytes Out 0
```

Step 8.4: Configure firewall policies to allow transit traffic from remote LAN to the local LAN (applicable only if firewall license is also enabled)

```
Black Box1/configure> firewall corp
Black Box1/configure/firewall corp> policy 1000 in address 10.0.2.0 24 10.0.1.0 24
Black Box1/configure/firewall corp/policy 1000 in> exit
Black Box1/configure/firewall corp> exit
```

Step 8.5: Display firewall policies in the corp map (applicable only if firewall license is enabled)

```
Black Box1> show firewall policy corp
Advanced: S - Self Traffic, F - Ftp-Filter, H - Http-Filter,
          R - Rpc-Filter, N - Nat-Ip/Nat-Pool, L - Logging,
          E - Policy Enabled, M - Smtp-Filter

Pri  Dir Source Addr        Destination Addr   Sport Dport Proto Action Advanced
---  --- -----------        ----------------   ----------------- ------ --------
1000 in  10.0.2.0/24        10.0.1.0/24        any   any   any   PERMIT E
1022 out any                any                any   any   any   PERMIT SE
1023 in  any                any                any   any   any   PERMIT SE
1024 out any                any                any   any   any   PERMIT E
```

Step 8.6: Display firewall policies in the corp map in detail (applicable only if firewall license is enabled)

```
Black Box1> show firewall policy corp detail

Policy with Priority 1000 is enabled, Direction is inbound
Action permit, Traffic is transit
Logging is disable
Source Address is 10.0.2.0/24, Dest Address is 10.0.1.0/24
Source Port is any, Dest Port is any, any
Schedule is disabled, Ftp-Filter is disabled
Smtp-Filter is disabled, Http-Filter is disabled
Rpc-Filter is disabled, Nat is disabled
Max-Connections 1024, Connection-Rate is disabled
Policing is disabled, Bandwidth is disabled
Bytes In 0, Bytes Out 0

Policy with Priority 1022 is enabled, Direction is outbound
Action permit, Traffic is self
Logging is disable
Source Address is any, Dest Address is any
Source Port is any, Dest Port is any, any
Schedule is disabled, Ftp-Filter is disabled
Smtp-Filter is disabled, Http-Filter is disabled
Rpc-Filter is disabled, Nat is disabled
Bytes In 0, Bytes Out 0

Policy with Priority 1023 is enabled, Direction is inbound
Action permit, Traffic is self
Logging is disable
Source Address is any, Dest Address is any
Source Port is any, Dest Port is any, any
Schedule is disabled, Ftp-Filter is disabled
Smtp-Filter is disabled, Http-Filter is disabled
Rpc-Filter is disabled, Nat is disabled
Bytes In 0, Bytes Out 0

Policy with Priority 1024 is enabled, Direction is outbound
Action permit, Traffic is transit
Logging is disable
Source Address is any, Dest Address is any
Source Port is any, Dest Port is any, any
Schedule is disabled, Ftp-Filter is disabled
Smtp-Filter is disabled, Http-Filter is disabled
Rpc-Filter is disabled, Nat is disabled
Max-Connections 1024, Connection-Rate is disabled
Policing is disabled, Bandwidth is disabled
Bytes In 11258, Bytes Out 5813
```

Step 9: Repeat steps 1 - 8 with suitable modifications on Black Box2 prior to passing traffic.

Step 10: Test the IPSec tunnel between Black Box1 and Black Box2 by passing traffic from the 10.0.1.0 to the 10.0.2.0 network

Step 11: After transit traffic is passed through the tunnel, display the IKE and IPSec SA tables.
Use the `show crypto ike sa all` and `show crypto ipsec sa all` commands.

4.4 Example 3: Multiple IPSec Proposals: Tunnel Mode Between Two Black Box Security Gateways

The following example demonstrates how a security gateway can use multiple ipsec (phase2) proposals to form an IP security tunnel to join two private networks: 10.0.1.0/24 and 10.0.2.0/24.

IKE Proposal offered by both Black Box1 and Black Box2:

- Phase 1: 3DES and SHA1

IPSec Proposals offered by Black Box1:

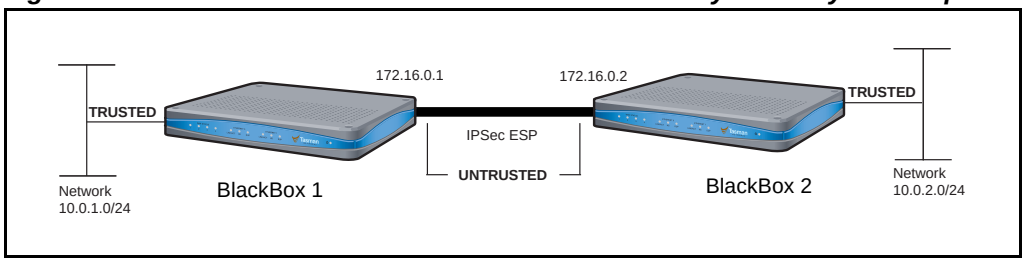
- Phase 2: Proposal1: IPSec ESP with DES and HMAC-SHA1
- Phase 2: Proposal2: IPSec ESP with AES (256-bit) and HMAC-SHA1

IPSec Proposal offered by Black Box2:

- Phase 2: Proposal1: IPSec ESP with AES (256-bit) and HMAC-SHA1

In this example, the Black Box1 router offers two IPSec proposals to the peer while the Black Box2 router offers only one proposal. As a result of quick mode negotiation, the two routers are expected to converge on a mutually acceptable proposal, which is the proposal “IPSec ESP with AES (256-bit) and HMAC-SHA1” in this example.

Figure 10 Tunnel Mode Between Two Black Box Security Gateways - Multiple Proposals



Step 1: Configure a WAN bundle of network type untrusted

```
Black Box1/configure/interface/bundle wan1> link t1 1
Black Box1/configure/interface/bundle wan1> encapsulation ppp
Black Box1/configure/interface/bundle wan1> ip address 172.16.0.1 24
Black Box1/configure/interface/bundle wan1> crypto untrusted
Black Box1/configure/interface/bundle wan1> exit
```

Step 2: Configure the Ethernet interface with trusted network type

```
Black Box1/configure> interface ethernet 0
  message: Configuring existing Ethernet interface
Black Box1/configure interface/ethernet 0> ip address 10.0.1.1 24
Black Box1/configure/interface/ethernet 0> crypto trusted
Black Box1/configure/interface/ethernet 0> exit
```

Step 3: Display the crypto interfaces

```
Blackbox> show crypto interfaces

Interface      Network
Name           Type
---------      -------
wan1           Untrusted
ethernet0      trusted

Blackbox>
```

Step 4: Add route to peer LAN

```
Black Box1/configure> ip route 10.0.2.0 24 wan1
```

Step 5: Configure IKE to the peer gateway

```
Black Box1/configure> crypto ike policy Black Box2 172.16.0.2
Black Box1/configure/crypto/ike/policy/Black Box2 172.16.0.2> local-address 172.16.0.1
  message: Default proposal created with priority1-des-sha-pre_shared-g1.
  message: Key String has to be configured by the user.
Black Box1/configure/crypto/ike/policy Black Box2 172.16.0.2> key secretkey
Black Box1/configure/crypto/ike/policy Black Box2 172.16.0.2> proposal 1
Black Box1/configure/crypto/ike/policy Black Box2 172.16.0.2/proposal 1> encryption-algorithm
3des-cbc
Black Box1/configure/crypto/ike/policy Black Box2 172.16.0.2/proposal 1> exit
Black Box1/configure/crypto/ike/policy Black Box2 172.16.0.2> exit
Black Box1/configure/crypto> exit
Black Box1/configure>
```

Step 6: Display IKE policies

```
Blackbox> show crypto ike policy all

Policy     Peer            Mode       Transform
------     ----            ----       ---------
Black Box 172.14.0.2     Main        P1 pre-g1-3des-sha

Blackbox>
```

Step 7: Configure IPSec tunnel to the remote host

```
Black Box1/configure>crypto ipsec policy Black Box2 172.16.0.2
Black Box1/configure/crypto/ipsec/policy Black Box2 172.16.0.2> match address 10.0.1.0 24
10.0.2.0 24
  message: Default proposal created with priority1-esp-3des-sha1-tunnel and activated.
Black Box1/configure/crypto/ipsec/policy Black Box2 172.16.0.2> proposal 1
Black Box1/configure/crypto/ipsec/policy Black Box2 172.16.0.2/proposal 1>
encryption-algorithm des-cbc
Black Box1/configure/crypto/ipsec/policy Black Box2 172.16.0.2/proposal 1> exit
Black Box1/configure/crypto/ipsec/policy Black Box2 172.16.0.2> proposal 2
  message: Proposal added with priority2-esp-3des-sha1-tunnel.
```

```
Black Box1/configure/crypto/ipsec/policy Black Box2 172.16.0.2/proposal 2>
encryption_algorithm aes256-cbc
Black Box1/configure/crypto/ipsec/policy Black Box2 172.16.0.2/proposal 2> exit
Black Box1/configure/crypto/ipsec/policy Black Box2 172.16.0.2> exit
Black Box1/configure/crypto> exit
Black Box1/configure>
```

Step 8: Display the IPSec policies

Use the `show crypto ipsec policy all` command.

Step 9: Repeat steps 1 - 8 with suitable modifications on Black Box2 prior to passing bi-directional traffic.

Step 10: Test the IPSec tunnel between Black Box1 and Black Box2 by passing traffic from the 10.0.1.0 network to the 10.0.2.0 network

Step 11: After traffic is passed through the tunnel, display the IKE and IPSec SA tables.

Use the `show crypto ike sa all` and `show crypto ipsec sa all` commands.

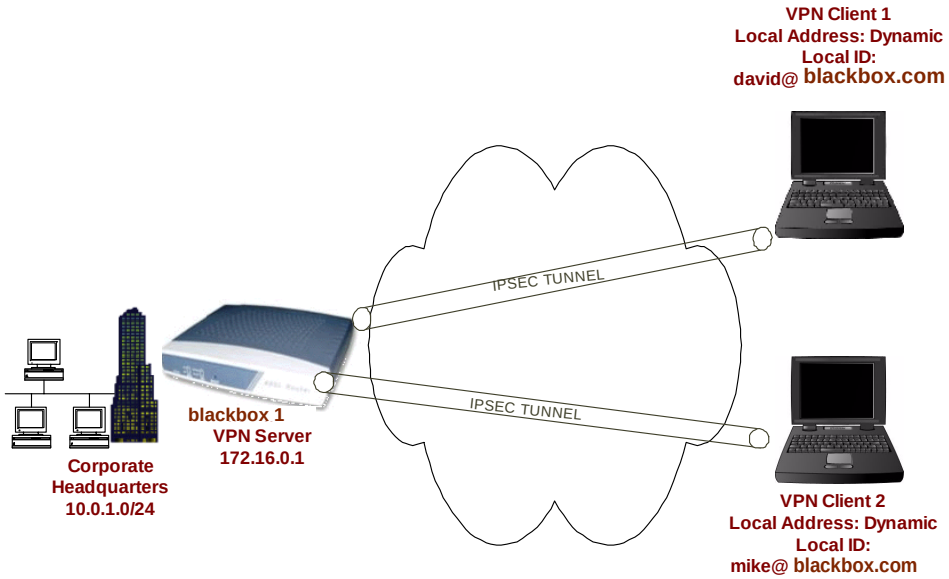
4.5 Example 4: IPSec remote access to corporate LAN using user group method

The following example demonstrates how to configure a Black Box router to be an IPSec VPN server using user group method with extended authentication (XAUTH) for remote VPN clients. The client could be any standard IPSec VPN client.

In this example, the client needs to access the corporate private network 10.0.1.0/24 through the VPN tunnel. The security requirements are as follows:

Phase 1: 3DES with SHA1, Xauth (Radius PAP)

Phase 2: IPSec ESP tunnel with AES256 and HMAC-SHA1



Step 1: As in Step1 of Example 1

Step 2: As in Step2 of Example 1

Step 3: As in Step3 of Example 1

Step 4: Configure dynamic IKE policy for a group of mobile users

```
Black Box1/configure> crypto
Black Box1/configure/crypto> dynamic
Black Box1/configure/crypto/dynamic> ike policy sales
Black Box1/configure/crypto/dynamic/ike/policy sales> local-address 172.16.0.1
Black Box1/configure/crypto/dynamic/ike/policy sales> remote-id email-id david@BlackBox.com
david
```

A new user david is added to the group sales. The default proposal created with priority1-des-sha1-pre_shared-g1 and the Key String has to be configured by the user.

```
Black Box1/configure/crypto/dynamic/ike/policy sales> remote-id email-id mike@BlackBox.com
New user mike is added to the group sales

Black Box1/configure/crypto/dynamic/ike/policy sales> key secretkeyforsalesusers
Black Box1/configure/crypto/dynamic/ike/policy sales> proposal 1
Black Box1/configure/crypto/dynamic/ike/policy sales/proposal 1> encryption-algorithm
3des-cbc
Black Box1/configure/crypto/dynamic/ike/policy sales/proposal 1> exit
Black Box1/configure/crypto/dynamic/ike/policy sales> client authentication radius pap
Black Box1/configure/crypto/dynamic/ike/policy sales> exit
Black Box1/configure/crypto/dynamic>
```

Step 5: Display dynamic IKE policies

```
Black Box1> show crypto dynamic ike policy all

Policy     Remote-id       Mode       Transform            Address-Pool
------     ---------       ----       ---------            ------------
sales      U david@Blackbox... Aggressive P1 pre-g1-3des-sha1
```

Step 6: Display dynamic IKE policies in detail

```
Black Box1> show crypto dynamic ike policy all detail

Policy name sales, User group name sales
Aggressive mode, Response Only, PFS is not enabled, Shared Key is *****
Client authentication is Radius(PAP)
Local addr: 172.16.0.1, Local ident 172.16.0.1 (ip-address)
Remote idents are david@Blackbox.com (email-id), mike@Blackbox.com (
email-id)

Proposal of priority 1
        Encryption algorithm: 3des
        Hash Algorithm: sha1
        Authentication Mode: pre-shared-key
        DH Group: group1
        Lifetime in seconds: 86400
           Lifetime in kilobytes: unlimited
```

Step 7: Configure dynamic IPSec policy for a group of mobile users

```
Black Box1/configure/crypto/dynamic> ipsec policy sales

Black Box1/configure/crypto/dynamic/ipsec/policy sales> match address 10.0.1.0 24
Default proposal created with priority1-esp-3des-sha1-tunnel and activated.

Black Box1/configure/crypto/dynamic/ipsec/policy sales> proposal 1
Black Box1/configure/crypto/dynamic/ipsec/policy sales/proposal 1> encryption-algorithm
aes256-cbc
Black Box1/configure/crypto/dynamic/ipsec/policy sales/proposal 1> exit
Black Box1/configure/crypto/dynamic/ipsec/policy sales> exit
Black Box1/configure/crypto/dynamic>
```

Step 8: Display dynamic IPSec policies

```
Black Box1> show crypto dynamic ipsec policy all

Policy     Match                    Proto Transform
------     -----                    ----- ---------
sales      S 10.0.1.0/24/any         Any  P1 esp-aes-sha1-tunl
           D any/any/any
INsales    S any/any/any             Any  P1 esp-aes-sha1-tunl
             D 10.0.1.0/24/any
```

Step 9: Display dynamic IPSec policies in detail

```
Black Box1> show crypto dynamic ipsec policy all detail

Policy sales is enabled, User group name sales
Direction is outbound, Action is Apply
Key Management is Automatic
PFS Group is disabled
Match Address:
        Protocol is Any
        Source ip address (ip/mask/port): (10.0.1.0/255.255.255.0/any)
        Destination ip address (ip/mask/port): (any/any/any)

Proposal of priority 1
        Protocol: esp
        Mode: tunnel
        Encryption Algorithm: aes256(key length=256 bits)
        Hash Algorithm: sha1
        Lifetime in seconds: 3600
        Lifetime in Kilobytes: 4608000


Policy INsales is enabled, User group name sales
Direction is inbound, Action is Apply
Key Management is Automatic
PFS Group is disabled
Match Address:
        Protocol is Any
        Source ip address (ip/mask/port): (any/any/any)
        Destination ip address (ip/mask/port): (10.0.1.0/255.255.255.0/any)

Proposal of priority 1
        Protocol: esp
        Mode: tunnel
        Encryption Algorithm: aes256(key length=256 bits)
        Hash Algorithm: sha1
        Lifetime in seconds: 3600
           Lifetime in Kilobytes: 4608000
```

Step 10: Configure radius server (applicable only if client authentication is configured in dynamic IKE policy)

```
Black Box1/configure> aaa
Black Box1/configure/aaa> radius
Black Box1/configure/aaa/radius> primary_server 172.168.2.1
Primary Radius server configured.
Black Box1/configure/aaa/radius> secondary_server 192.168.2.1
Secondary Radius server configured.
Black Box1/configure/aaa/radius> exit
Black Box1/configure/aaa> exit
```

Step 11: Configure firewall policies to allow IKE negotiation through untrusted interface (applicable only if firewall license is also enabled)

```
Black Box1/configure> firewall internet
Black Box1/configure/firewall internet> policy 1000 in service ike self
Black Box1/configure/firewall internet/policy 1000 in> exit
Black Box1/configure/firewall internet> exit
```

Step 12: Display firewall policies in the internet map (applicable only if firewall license is enabled)

```
Black Box1> show firewall policy internet
Advanced: S - Self Traffic, F - Ftp-Filter, H - Http-Filter,
          R - Rpc-Filter, N - Nat-Ip/Nat-Pool, L - Logging,
          E - Policy Enabled, M - Smtp-Filter

Pri  Dir Source Addr        Destination Addr   Sport Dport Proto Action Advanced
---  --- -----------        ----------------   ----------------- ------ --------
1000 in  any                any                ike               PERMIT SE
1024 out any                any                any   any   any   PERMIT SE
```

Step 13: Display firewall policies in the internet map in detail (applicable only if firewall license is enabled)

```
Black Box1> show firewall policy internet detail

Policy with Priority 1000 is enabled, Direction is inbound
Action permit, Traffic is self
Logging is disable
Source Address is any, Dest Address is any
Source Port is any, Service Name is ike
Schedule is disabled, Ftp-Filter is disabled
Smtp-Filter is disabled, Http-Filter is disabled
Rpc-Filter is disabled, Nat is disabled
Bytes In 0, Bytes Out 0

Policy with Priority 1024 is enabled, Direction is outbound
Action permit, Traffic is self
Logging is disable
Source Address is any, Dest Address is any
Source Port is any, Dest Port is any, any
Schedule is disabled, Ftp-Filter is disabled
Smtp-Filter is disabled, Http-Filter is disabled
Rpc-Filter is disabled, Nat is disabled
    Bytes In 0, Bytes Out 0
```

Step 14: Configure firewall policies for a group of mobile users to allow access to the local LAN (applicable only if firewall license is enabled)

```
Black Box1/configure/firewall corp>
Black Box1/configure/firewall corp> policy 1000 in user-group sales address any any 10.0.1.0
24
Black Box1/configure/firewall corp/policy 1000 in
>exit
Black Box1/configure/firewall corp>
```

Step 15: Display firewall policies in the corp map (applicable only if firewall license is enabled)

```
Black Box1> show firewall policy corp
Advanced: S - Self Traffic, F - Ftp-Filter, H - Http-Filter,
          R - Rpc-Filter, N - Nat-Ip/Nat-Pool, L - Logging,
          E - Policy Enabled, M - Smtp-Filter

Pri  Dir Source Addr        Destination Addr   Sport Dport Proto Action Advanced
---  --- -----------        ----------------   ----------------- ------ --------
1000 in  any                10.0.1.0/24        any   any   any   PERMIT E
1022 out any                any                any   any   any   PERMIT SE
1023 in  any                any                any   any   any   PERMIT SE
1024 out any              any               any   any   any   PERMIT E
```

Step 16: Display firewall policies in the corp map in detail (applicable only if firewall license is enabled)

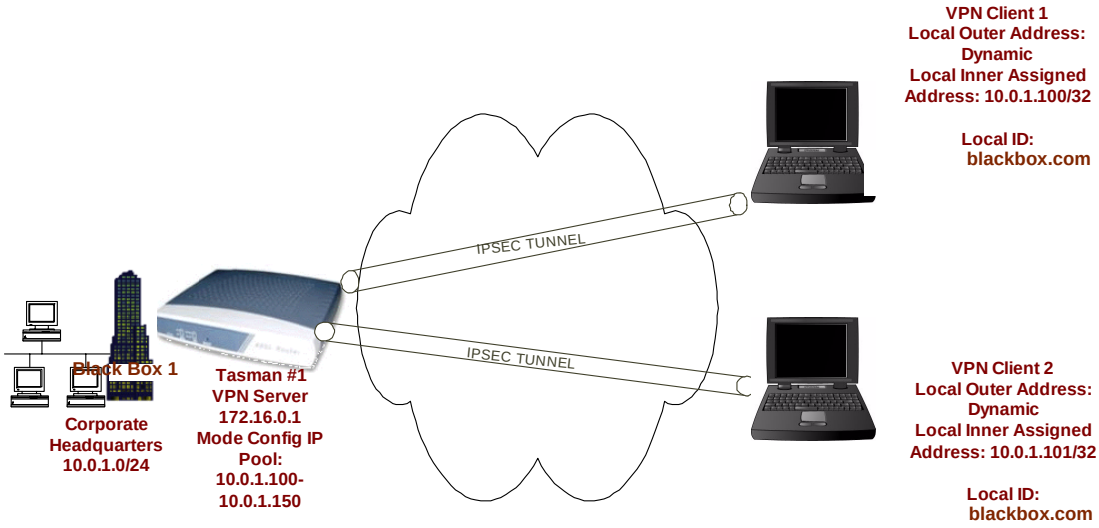
4.1Example 5: IPSec remote access to corporate LAN using mode configuration method

The following example demonstrates how to configure a Black Box router to be an IPSec VPN server using mode-configuration method. The client could be any standard mode configuration enabled IPSec VPN client.

In this example, the client needs to access the corporate private network 10.0.1.0/24 through the VPN tunnel. The server has a pool of ip addresses from 20.1.1.100 through 20.1.1.150 to be allocated for mode configuration enabled VPN clients. The assigned IP address will be used by the VPN client as the source address in the inner IP header. The outer IP header will carry the dynamic IP address assigned by the Internet Service Provider as the source address. The security requirements are as follows:

Phase 1: 3DES with SHA1, Mode Configuration

Phase 2: IPSec ESP tunnel with AES256 and HMAC-SHA1



Step 1: As in Step1 of Example 1

Step 2: As in Step2 of Example 1

Step 3: As in Step3 of Example 1

Step 4: Configure dynamic IKE policy for a group of mobile users

```
Black Box1/configure> crypto
Black Box1/configure/crypto> dynamic
Black Box1/configure/crypto/dynamic> ike policy sales modecfg-group
Black Box1/configure/crypto/dynamic/ike/policy sales> local-address 192.168.55.52

Black Box1/configure/crypto/dynamic/ike/policy sales> remote-id email david@Blackbox.com
```

The default proposal is created with priority1-des-sha1-pre_shared-g1, the Key String has to be configured by the user, and the default IPSec proposal 'sales' added with priority1-3des-sha1-tunnel.

```
Black Box1/configure/crypto/dynamic/ike/policy sales> remote-id email mike@Blackbox.com
Black Box1/configure/crypto/dynamic/ike/policy sales> key secretkeyforsales
Black Box1/configure/crypto/dynamic/ike/policy sales> proposal 1
Black Box1/configure/crypto/dynamic/ike/policy sales/proposal 1> encryption-algorithm
3des-cbc
Black Box1/configure/crypto/dynamic/ike/policy sales/proposal 1> exit
Black Box1/configure/crypto/dynamic/ike/policy sales> client configuration
Black Box1/configure/crypto/dynamic/ike/policy sales/client/configuration> address-
pool 1 20.1.1.100 20.1.1.150
Black Box1/configure/crypto/dynamic/ike/policy sales/client/configuration> exit
Black Box1/configure/crypto/dynamic/ike/policy sales> exit
Black Box1/configure/crypto/dynamic> exit
```

Step 5: Display dynamic IKE policies

```
Black Box1> show crypto dynamic ike policy all

Policy     Remote-id       Mode       Transform            Address-Pool
------     ---------       ----       ---------            ------------
sales      U david@BlackBox... Aggressive P1 pre-g1-3des-sha1  1 S 20.1.1.100

E20.1.1.150
```

Step 6: Display dynamic IKE policies in detail

```
Black Box1> show crypto dynamic ike policy all detail

Policy name sales, Modeconfig group
Aggressive mode, Response Only, PFS is not enabled, Shared Key is *****
Local addr: 192.168.55.52, Local ident 192.168.55.52 (ip-address)
Remote idents are david@Blackbox.com (email-id), mike@Blackbox.com (email-id)
Address Pool:
        Pool# 1: 20.1.1.100 to 20.1.1.150

Proposal of priority 1
        Encryption algorithm: 3des
        Hash Algorithm: sha1
        Authentication Mode: pre-shared-key
        DH Group: group1
        Lifetime in seconds: 86400
        Lifetime in kilobytes: unlimited
```

Step 7: Configure dynamic IPSec policy for a group of mobile users

```
Black Box1/configure/crypto>
Black Box1/configure/crypto> dynamic
Black Box1/configure/crypto/dynamic> ipsec policy sales modecfg-group
Black Box1/configure/crypto/dynamic/ipsec/policy sales> match address 10.0.1.0 24
Black Box1/configure/crypto/dynamic/ipsec/policy sales> proposal 1
Black Box1/configure/crypto/dynamic/ipsec/policy sales/proposal 1> encryption-algorithm
aes256-cbc
Black Box1/configure/crypto/dynamic/ipsec/policy sales/proposal 1> exit
Black Box1/configure/crypto/dynamic/ipsec/policy sales> exit
Black Box1/configure/crypto/dynamic> exit
```

Step 8: Display dynamic IPSec policies

```
Black Box1> show crypto dynamic ipsec policy all

Policy     Match                    Proto Transform
------     -----                    ----- ---------
sales      S 10.0.1.0/24/any         Any  P1 esp-aes-sha1-tunl
                    D any/any/any
```

Step 9: Display dynamic IPSec policies in detail

```
Black Box1> show crypto dynamic ipsec policy all detail

Policy sales is enabled, Modeconfig Group
Action is Apply
Key Management is Automatic
PFS Group is disabled
Match Address:
        Protocol is Any
        Source ip address (ip/mask/port): (10.0.1.0/255.255.255.0/any)
        Destination ip address (ip/mask/port): (any/any/any)

Proposal of priority 1
        Protocol: esp
        Mode: Tunnel
        Encryption Algorithm: aes256(key length=256 bits)
        Hash Algorithm: sha1
        Lifetime in seconds: 3600
        Lifetime in Kilobytes: 4608000
```

Step 10: Configure firewall policies to allow IKE negotiation through untrusted interface (applicable only if firewall license is also enabled)

```
Black Box1/configure> firewall internet
Black Box1/configure/firewall internet> policy 1000 in service ike self
Black Box1/configure/firewall internet/policy 1000 in> exit
Black Box1/configure/firewall internet> exit
```

Step 11: Display firewall policies in the internet map (applicable only if firewall license is enabled)

```
Black Box1> show firewall policy internet
Advanced: S - Self Traffic, F - Ftp-Filter, H - Http-Filter,
          R - Rpc-Filter, N - Nat-Ip/Nat-Pool, L - Logging,
          E - Policy Enabled, M - Smtp-Filter

Pri  Dir Source Addr        Destination Addr   Sport Dport Proto Action Advanced
---  --- -----------        ----------------   ----------------- ------ --------
1000 in  any                any                ike               PERMIT SE
1024 out any                any                any   any   any   PERMIT SE
```

Step 12: Display firewall policies in the internet map in detail (applicable only if firewall license is enabled)

```
Black Box1> show firewall policy internet detail

Policy with Priority 1000 is enabled, Direction is inbound
Action permit, Traffic is self
Logging is disable
Source Address is any, Dest Address is any
Source Port is any, Service Name is ike
Schedule is disabled, Ftp-Filter is disabled
Smtp-Filter is disabled, Http-Filter is disabled
Rpc-Filter is disabled, Nat is disabled
Bytes In 0, Bytes Out 0

Policy with Priority 1024 is enabled, Direction is outbound
Action permit, Traffic is self
Logging is disable
Source Address is any, Dest Address is any
Source Port is any, Dest Port is any, any
Schedule is disabled, Ftp-Filter is disabled
Smtp-Filter is disabled, Http-Filter is disabled
Rpc-Filter is disabled, Nat is disabled
Bytes In 0, Bytes Out 0
```

Step 13: Configure firewall policies for a group of mobile users to allow access to the local LAN (applicable only if firewall license is enabled)

```
Black Box1/configure> firewall corp
Black Box1/configure/firewall corp> policy 1000 in address 20.1.1.100 20.1.1.150
10.0.1.0 24
Black Box1/configure/firewall corp/policy 1000 in
>exit
```

Step 14: Display firewall policies in the corp map (applicable only if firewall license is enabled)

```
Black Box1> show firewall policy corp
Advanced: S - Self Traffic, F - Ftp-Filter, H - Http-Filter,
          R - Rpc-Filter, N - Nat-Ip/Nat-Pool, L - Logging,
          E - Policy Enabled, M - Smtp-Filter

Pri  Dir Source Addr        Destination Addr   Sport Dport Proto Action Advanced
---  --- -----------        ----------------   ----------------- ------ --------
1000 in  20.1.1.100         10.0.1.0/24        any   any   any   PERMIT E
         20.1.1.150
1022 out any                any                any   any   any   PERMIT SE
1023 in  any                any                any   any   any   PERMIT SE
1024 out any                any                any   any   any   PERMIT E
```

Step 15: Display firewall policies in the corp map in detail (applicable only if firewall license is enabled)

```
Black Box1> show firewall policy corp detail

Policy with Priority 1000 is enabled, Direction is inbound
Action permit, Traffic is transit
Logging is disable
Source Address is 20.1.1.100-20.1.1.150, Dest Address is 10.0.1.0/24
Source Port is any, Dest Port is any, any
Schedule is disabled, Ftp-Filter is disabled
Smtp-Filter is disabled, Http-Filter is disabled
Rpc-Filter is disabled, Nat is disabled
Max-Connections 1024, Connection-Rate is disabled
Policing is disabled, Bandwidth is disabled
Bytes In 0, Bytes Out 0

Policy with Priority 1022 is enabled, Direction is outbound
Action permit, Traffic is self
Logging is disable
Source Address is any, Dest Address is any
Source Port is any, Dest Port is any, any
Schedule is disabled, Ftp-Filter is disabled
Smtp-Filter is disabled, Http-Filter is disabled
Rpc-Filter is disabled, Nat is disabled
Bytes In 0, Bytes Out 0

Policy with Priority 1023 is enabled, Direction is inbound
Action permit, Traffic is self
Logging is disable
Source Address is any, Dest Address is any
Source Port is any, Dest Port is any, any
Schedule is disabled, Ftp-Filter is disabled
Smtp-Filter is disabled, Http-Filter is disabled
Rpc-Filter is disabled, Nat is disabled
Bytes In 0, Bytes Out 0

Policy with Priority 1024 is enabled, Direction is outbound
Action permit, Traffic is transit
Logging is disable
Source Address is any, Dest Address is any
Source Port is any, Dest Port is any, any
Schedule is disabled, Ftp-Filter is disabled
Smtp-Filter is disabled, Http-Filter is disabled
Rpc-Filter is disabled, Nat is disabled
Max-Connections 1024, Connection-Rate is disabled
Policing is disabled, Bandwidth is disabled
Bytes In 11258, Bytes Out 5813
```

5
IPSEC SPECIFICATIONS

5.1IPSec Appendix

This appendix provides information about IPSec supported protocols and modes, encryption algorithms and block sizes, and Black Box IPSec and IKE default values.

IPSec Supported Protocols and Algorithms
The following tables provide supported protocol and algorithm information.

Table 1 IPSec Protocols Support

Supported Security Protocols	Mode
ESP	Tunnel Transport
AH	Tunnel Transport

Table 2 Encryption Algorithms

Encryption Algorithms for ESP	Block Size
Data Encryption Standard (DES)	56-bits
Triple Data Encryption Standard (3DES)	168-bits
Advanced Encryption Standard (AES-128)	128-bits
Advanced Encryption Standard (AES-192)	192-bits
Advanced Encryption Standard (AES-256)	256-bits
Null Encryption	

Table 3 Authentication Algorithms

Authentication Algorithms for AH/ESP	Hash Size
HMAC-MD5-96	96-bits

HMAC-HSHA1-96	96-bits

Table 4 Diffie-Hellman Groups

Diffie-Hellman Groups for Authentication	Key Size
Group 1	768-bits
Group 2	1024-bits

5.1.1 Black Box IKE and IPSec Defaults

To minimize configuration required by the user, default IKE and IPSec values have been implemented in Black Box's encryption scheme.

5.1.1.1 IKE Defaults

The following table lists IKE defaults. When the user creates an IKE policy specifying an IKE peer, an IKE proposal with priority 1 is automatically created. However, to make the IKE policy fully functional, the user must enter a pre-shared key.

Figure 11 IKE Default Values

Parameter Name	Black Box Default Value
Mode	Main mode
Perfect forward secrecy	Disabled
Hash algorithm	SHA1
Encryption algorithm	DES
Authentication method	PreShared
DH Group	Group 1
Lifetime	86400 seconds
Response type	Initiator and responder

5.1.1.2 IPSec Defaults

The following table lists IPSec defaults. When the user creates an IPSec policy and provides the match address, an IPSec proposal with priority 1 is automatically created. When an outbound policy is specified, an inbound policy is automatically created.

Figure 12 IPSec Default Values

Parameter Name	Black Box Default Value
Key management type	Automatic
Hash algorithm	SAH1
Encryption algorithm	3DES
Protocol	ESP
Mode	Tunnel
Lifetime	3600 seconds
Direction	Out
Position in SPD where policy added	End
Perfect forward secrecy	Disabled

6
FORWARDING IP TRAFFIC

6.1IP Multiplexing

IP Multiplexing is a method for the transparent forwarding of IP packets between LAN and WAN interfaces. LAN to WAN forwarding is accomplished through a Proxy ARP process. A Black Box system maps a unique MAC address to each WAN link then responds with this MAC address when a device on the LAN broadcasts an ARP request for a remote device. These MAC addresses serve as “tags” for forwarding packets received on the LAN. WAN to LAN and WAN to WAN forwarding is based on configured forwarding entries.

IP Multiplexing differs from bridging and switching in that it does not flood traffic or perform address learning. IP Multiplexing devices differ from routers in that they do not appear as a router hop, and they cannot be specified as a default router/gateway on a LAN.

6.1.1 Packet Forwarding Modes

There are two modes for WAN to LAN and WAN to WAN packet forwarding

- IP Routes – Forwarding based on routing statements, both specific and default.
- Source Forwarding – Forwards all traffic arriving on a specified WAN bundle to a specified device on the LAN.

The following table provides information about applications and a suggested forwarding mode for each.

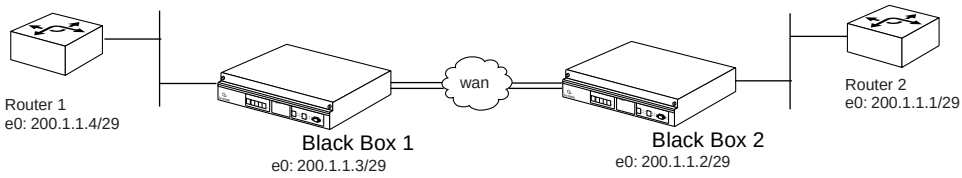
Table 5 Applications and Suggested Forwarding Modes

Application	Suggested Forwarding Mode
Forwarding traffic from different WAN links to separate routers on the LAN	Source Forwarding
Forwarding all WAN traffic to a single router on the LAN	Default IPMux Routes
Forwarding to both LAN and WAN router	Specific IPMux Routes

6.1.2 Proxy ARP and Packet Forwarding

In the simple network example below, router 1, router 2, and both Black Box Ethernets are on a single 29-bit IP subnet. Consider the sequence that occurs when router 1 pings router 2.

Figure 13 Proxy ARP and Packet Forwarding



1. Router 1 broadcasts an ARP request for 200.1.1.1.
2. Black Box 1 recognizes that router 200.1.1.1 is reachable via its WAN interface, based on a configured IP route.
3. Black Box 1 Proxy ARPs, responding with the MAC address mapped to bundle WAN1.
4. Router 1 unicasts the ping echo request to that MAC address.
5. Black Box 1 forwards the echo request for 200.1.1.1 through the WAN1 bundle.
6. Black Box 2 receives a packet on WAN2 and forwards it to directly connected router 2.
7. The echo reply from router 2 to router 1 is returned in the same manner.

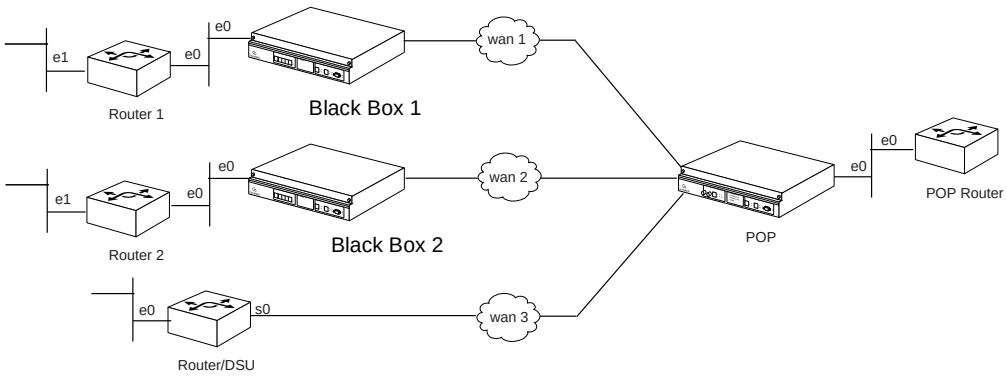
6.1.3 Addressing in IP Multiplexing Networks

IP addressing in an IP Multiplexing design must take into account the fact that the router on the LAN must see the remote router as residing on the same LAN or IP network. There are a number of addressing schemes that can fulfill this requirement, including:

- Single subnet
- Split subnet
- Secondary addressing

Consider the following network, consisting of three remote sites. Two remote sites utilize Black Box equipment, while the third is a simple router/dsu combination. Five IP addressing schemes are provided below, all refer to the following network.

Figure 14 Addressing in IP Multiplexing Networks



6.1.4 Single Subnet

The emphasis in the single subnet approach is that all seven devices have interfaces in a single 28-bit subnet 192.1.1.0 / 28. The WAN addressing utilizes reserved address space.

Table 6 Single Subnet Addressing

POP Router	e0:	192.1.1.1/28
POP Black Box	e0:	192.1.1.2/28
	wan1:	10.1.1.1/30
	wan2:	10.1.1.5/30
	wan3:	10.1.1.9/30
Black Box 1	e0:	192.1.1.3/28
	wan1:	10.1.1.2/30
Router 1	e0:	192.1.1.4/28
Black Box 2	e0:	192.1.1.5/28
	wan1:	10.1.1.6/30
Router 2	e0:	192.1.1.6/28
Router/DSU	s0:	192.1.1.7/28

6.1.5 Split Subnet

This is similar to the single subnet scheme in that all four routers are in the same 28-bit subnet, but the Black Box products are on smaller, 30-bit subnets.

Table 7 Split Subnet Addressing

POP Router	e0:	192.1.1.1/28
POP Black Box	e0:	192.1.1.2/30
	wan1:	10.1.1.1/30
	wan2:	10.1.1.5/30
	wan3:	10.1.1.9/30
Black Box 1	e0:	192.1.1.5/30
	wan1:	10.1.1.2/30
Router 1	e0:	192.1.1.6/28
Black Box 2	e0:	192.1.1.9/30
	wan1:	10.1.1.6/30
Router 2	e0:	192.1.1.10/28
Router/DSU	s0:	192.1.1.14/28

6.1.6 Secondary Addressing – POP Only

Secondary addressing approaches rely on configuring the POP router with a secondary Ethernet address for each remote site. The POP-only approach uses secondary addresses at the POP while the remote router utilizes only a primary address.

Table 8 POP Only Secondary Addressing

POP Router	e0:	200.1.1.1/30 primary
		199.1.1.1/29 secondary
		199.1.1.9/29 secondary
		199.1.1.17/29 secondary
POP Black Box	e0:	200.1.1.2/30
	wan1:	10.1.1.1/24
	wan2:	10.1.2.1/24
	wan3:	10.1.3.1/24
Black Box 1	e0:	199.1.1.2/29
	wan1:	10.1.1.2/24
Router 1	e0:	199.1.1.3/29
Black Box 2	e0:	199.1.1.10/29
	wan1:	10.1.2.2/24
Router 2	e0:	199.1.1.11/29
Router/DSU	s0:	199.1.1.18/29

6.1.7 Secondary Addressing – 30 Bit

This approach relies on configuring the POP router with a secondary Ethernet address for each remote site. The remote router is also configured with a secondary address in that same subnet. The 30-bit approach uses reserved addresses for bundle addressing. The router primary and the directly connected Black Box reside in a different 30-bit subnet.

Table 9 30-Bit Secondary Addressing

POP Router	e0:	200.1.1.1/30 primary
		199.1.1.1/30 secondary
		199.1.1.5/30 secondary
		199.1.1.9/30 secondary
POP Black Box	e0:	200.1.1.1/30
	wan1:	10.1.1.1/30
	wan2:	10.1.1.5/30
	wan3:	10.1.1.9/30
Black Box 1	e0:	201.1.1.2/30
	wan1:	10.1.1.2/30
Router 1	e0:	201.1.1.1/30 primary
		199.1.1.2/30 secondary
Black Box 2	e0:	202.1.1.2/30
	wan1:	10.1.1.6/30
Router 2	e0:	202.1.1.1/30 primary
		199.1.1.6/30 secondary
Router/DSU	s0:	199.1.1.10/30

6.1.8 Secondary Addressing – 29 Bit

This approach utilizes a 29-bit subnet for each remote connection. Within each 29-bit subnet is the POP router secondary, the Black Box WAN addressing, and the remote router secondary.

POP Router	e0:	200.1.1.1/30 primary 199.1.1.1/29 secondary 199.1.1.9/29 secondary 199.1.1.17/29 secondary
POP Black Box	e0: wan1: wan2: wan3:	200.1.1.2/30 199.1.1.2/29 199.1.1.10/29 199.1.1.18/29
Black Box 1	e0: wan	201.1.1.2/30 199.1.1.3/29
Router 1	e0:	201.1.1.1/30 primary 199.1.1.4/29 secondary
Black Box 2	e0: wan1:	202.1.1.2/30 199.1.1.11/29
Router 2	e0:	202.1.1.1/30 primary 199.1.1.12/29 secondary
Router/DSU	s0:	199.1.1.19/29

6.1.9 Pros and Cons of Different IP Addressing Schemes

The following table provides information about addressing scheme pros and cons.

Table 10 Addressing Schemes: Pros and Cons

Approach	Pros	Cons
Single Subnet	Minimizes consumption of IP address space	POP Black Box requires two route statements per remote connection.
Split Subnet	Less routes required in Black Box	Consumes 29-bit subnet per remote site.
Secondary Addressing	Easily Scalable	Consumes 29-or 30-bit subnet per remote. Not transparent to certain routing protocols.

6.1.10 Routing Considerations for IP Multiplexing

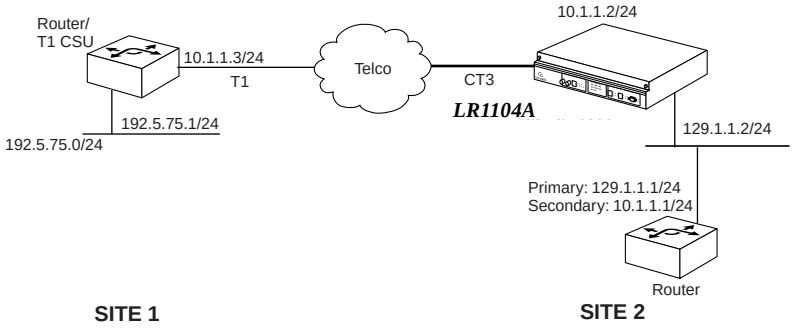
- RIP / RIP2 / IGRP –Turn off split horizons to enable routing updates through secondary addresses, if used.
- EIGRP – Updates are sourced only from primary addresses, although routers will listen to updates arriving on primary and secondary.
- OSPF – For Cisco and other routers, routing updates are sourced and detected only on primary addresses, therefore secondary addressing schemes are not usable.
- BGP4 – Routing updates are fully functional over primary and secondary addresses.

7
IP MULTIPLEXING HDLC CONFIGURATIONS

7.1Connecting a Black Box Router to a Router/CSU via HDLC

The following diagram details a single T1 connection between a Black Box and a remote router/CSU combination. Secondary IP addressing is used for IP multiplexing.

Figure 15 IP Multiplexing Application



The two sites communicate over a single T1 channel. The Site 2 WAN bundle, named “ToSite1”, consists of a single T1 channel coming in via a CT3 circuit. Site 1 router's default route is directed to the Site 2 router: **0.0.0.0/0 10.1.1.1**

The Site 2 router is configured with: primary ethernet address: **129.1.1.1/24**, secondary ethernet addr on the WAN subnet: **10.1.1.1/24**, and route to the Site 1 router: **192.5.75.0/24 10.1.1.3**.

7.1.1 Configure the Black Box LR1104A at Site 2

```
Site2-LR1104A> configure term
Site2-LR1104A/configure> interface ethernet 0
Site2-LR1104A/configure/interface/ethernet> ip addr 129.1.1.2 255.255.255.0
Site2-LR1104A/configure/interface/ethernet> exit

Site2-LR1104A/configure> interface bundle toSite1
Site2-LR1104A/configure/interface/bundle> link ct3 1 1
Site2-LR1104A/configure/interface/bundle> encap hdlc
Site2-LR1104A/configure/interface/bundle> ip addr 10.1.1.2 255.255.255.0
Site2-LR1104A/configure/interface/bundle> ipmux source_forwarding 129.1.1.1
Site2-LR1104A/configure/interface/bundle> exit
```

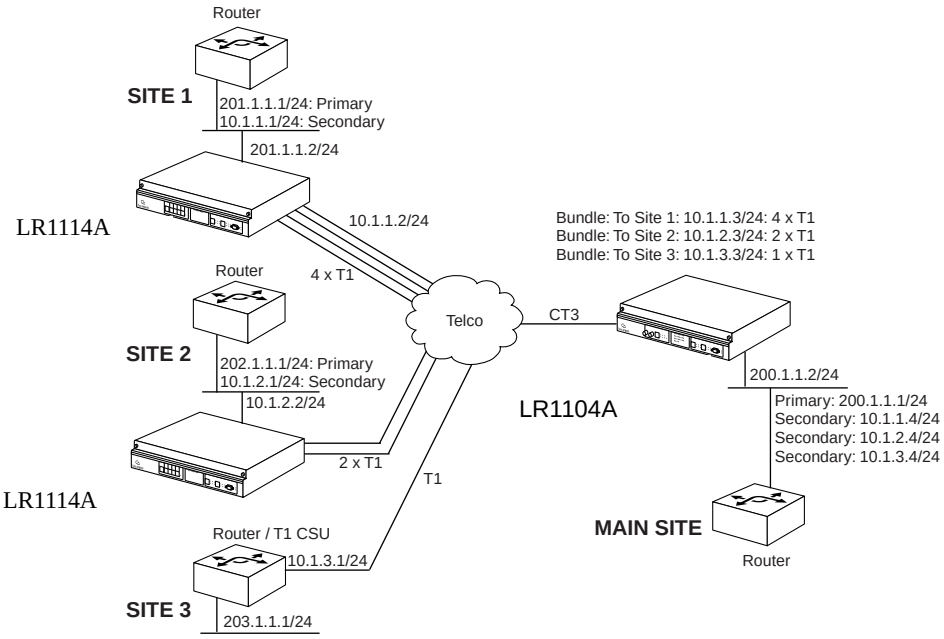
8
IP MULTIPLEXING PPP AND MLPPP CONFIGURATIONS

8.1Configuring Multiple PPP and MLPPP Bundles

The following figure shows a Black Box LR1104A at the main site communicating with three remote sites. Site 1 utilizes a Black Box LR1114A communicating over a 4 x T1 WAN bundle. Site 2 utilizes a Black Box LR1114A communicating over a 2 x T1 WAN bundle. Site 3 utilizes a router/T1 CSU combination to communicate over a single T1.

This example focuses on the main site Black Box LR1104A - refer to other configuration examples for details on remote site configurations. Secondary IP addressing is used for IP multiplexing in this example.

Figure 16 IP Multiplexing Application



The main site Black Box LR1104A is configured with three WAN bundles. Each bundle has a unique name and an IP address from a unique WAN subnet associated with it. The main site router is configured with the following IP routes: To Site 1 **201.1.1.0/24 10.1.1.1**, To Site 2 **202.1.1.0/24 10.1.2.1**, and To Site 3 **203.1.1.0/24 10.1.3.1**.

8.1.1 Configure the Black Box LR1104A at the Main Site

```
MainLR1104A/configure> interface ethernet 0
MainLR1104A/configure/interface/ethernet> ip addr 200.1.1.2 255.255.255.0
MainLR1104A/configure/interface/ethernet> exit

MainLR1104A/configure> module ct3 1
MainLR1104A/configure/module/ct3> t1 1-4 esf b8zs line gen_det description "4 x T1 to Site 1"
MainLR1104A/configure/module/ct3>exit
MainLR1104A/configure> interface bundle toSite1
MainLR1104A/configure/interface/bundle> link ct3 1 1-4
MainLR1104A/configure/interface/bundle> encap ppp
MainLR1104A/configure/interface/bundle> ip addr 10.1.1.3 255.255.255.0
MainLR1104A/configure/interface/bundle> ipmux source_forwarding 200.1.1.1
MainLR1104A/configure/interface/bundle> exit

MainLR1104A/configure> module ct3 1
MainLR1104A/configure/module/ct3> t1 5-6 esf b8zs line gen_det description "2 x T1 to Site 2"
MainLR1104A/configure/module/ct3>exit
MainLR1104A/configure> interface bundle toSite2
MainLR1104A/configure/interface/bundle> link ct3 1 5-6
MainLR1104A/configure/interface/bundle> encap ppp
MainLR1104A/configure/interface/bundle> ip addr 10.1.2.3 255.255.255.0
MainLR1104A/configure/interface/bundle> ipmux source_forwarding 200.1.1.1
MainLR1104A/configure/interface/bundle> exit

MainLR1104A/configure> module ct3 1
MainLR1104A/configure/module/ct3> t1 7 esf b8zs line gen_det description "T1 to Site 3"
MainLR1104A/configure/module/ct3> exit
MainLR1104A/configure> interface bundle toSite3
MainLR1104A/configure/interface/bundle> link ct3 1 7
MainLR1104A/configure/interface/bundle> encap ppp
MainLR1104A/configure/interface/bundle> ip addr 10.1.3.3 255.255.255.0
MainLR1104A/configure/interface/bundle> ipmux source_forwarding 200.1.1.1
MainLR1104A/configure/interface/bundle> exit
```

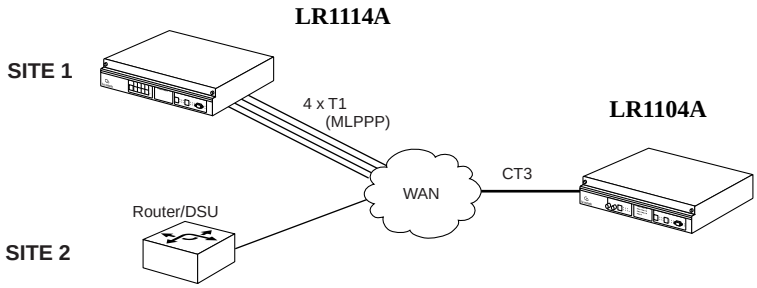
9 CONFIGURING PPP, MLPPP, AND HDLC

9.1Layer Two Configurations: PPP, MLPPP, and HDLC

Black Box systems may be configured for a variety of Layer 2 protocols. This document outlines High-level Data Link Control (HDLC), Point to Point Protocol (PPP), and Multilink PPP (MLPPP) configurations. Other Black Box documents outline Frame Relay and Multilink Frame Relay configuration.

Black Box LR1104A systems are often used at POPs to aggregate data for WAN transmission. The following figure details PPP and multilink PPP connections from two CPE sites to a main site.

Figure 17 PPP/MLPPP Application



Site 1 uses a Black Box LR1114A system to establish a 6 Mbps MLPPP connection (four T1 lines) to the main site. In this example, MLPPP segmentation is configured lower than the default setting of 512 bytes, and the differential delay tolerance is tighter than the default 128 milliseconds.

Site 2 connects to the main site over a single T1 link with PPP encapsulation. The LR1104A system PPP parameters (i.e., the maximum transmit and receive byte sizes) are adjusted to comply with the Site 1 router configuration.

9.1.1 MLPPP Configuration

9.1.1.1 Configure the Black Box LR1114A System at Site 1

```
Blackbox> configure term
Blackbox/configure> interface bundle ToMain
Blackbox/configure/interface/bundle> link t1 1-4
```

NOTE

MLPPP is not explicitly configured via the encapsulation command. Instead, multilink PPP is automatically invoked when a bundle with PPP encapsulation has two or more T1 links.

```
Blackbox/configure/interface/bundle> encap ppp
Blackbox/configure/interface/bundle> mlppp seg_threshold LR1114A differential_delay
50
Blackbox/configure/interface/bundle> ip addr 192.168.1.2 255.255.255.0
Blackbox/configure/interface/bundle> exit
```

9.1.2 PPP and MLPPP Configuration

9.1.2.1 Configure the Black Box LR1104A System at the Main Site

```
Blackbox/configure> interface bundle ToSite1
Blackbox/configure/interface/bundle> link ct3 1 5-8
Blackbox/configure/interface/bundle> encap ppp
Blackbox/configure/interface/bundle> mlppp seg_threshold LR1114A differential_delay
50
Blackbox/configure/interface/bundle> ip addr 192.168.1.1 255.255.255.0
Blackbox/configure/interface/bundle> exit

Blackbox/configure> interface bundle ToSite2
Blackbox/configure/interface/bundle> link ct3 1 9
Blackbox/configure/interface/bundle> encap ppp
Blackbox/configure/interface/bundle> ppp mtu 100-250-1000 mru 100-250-1000
Blackbox/configure/interface/bundle> ip addr 192.168.2.1 255.255.255.0
Blackbox/configure/interface/bundle> exit
```

9.1.3 HDLC Configuration

HDLC encapsulation may be substituted for PPP between the main site and site 2

9.1.3.1 Configure the Black Box LR1104A System at the Main Site

```
Blackbox/configure> interface bundle ToSite2
Blackbox/configure/interface/bundle> link ct3 1 9
Blackbox/configure/interface/bundle> encap hdlc
Blackbox/configure/interface/bundle> hdlc keepalive 20
Blackbox/configure/interface/bundle> ip addr 192.168.2.1 255.255.255.0
Blackbox/configure/interface/bundle> exit
```

NOTE

In the above command sequence, the HDLC keepalive time interval was changed from its default setting of 10 seconds to 20 seconds

10
CONFIGURING FIREWALLS

10.1Firewalls

Configuring firewalls allows administrators to adapt network protection policies to meet ever-changing hacker and intruder threats. Just as virus protection software requires updates to protect against the latest intrusion attacks, firewalls must be updated. In this release of Black Box software, administrators are able to filter traffic on specific ports, protect against Denial of Services attacks, enable IP packet reassembly, and so forth.

There are three licenses that control access to the features:

- Basic VPN Management (`vpn_mgmt`)—allows users to manage a remote Black Box router.
- Firewall (`firewall`)—allows users to manage the firewall features. Also includes Basic VPN Management.
- Advanced VPN and firewall (`vpn_plus_firewall`)—Allows users to manage remote LANs. Also includes Basic VPN and Firewall licenses.

To see the licenses available in this release, enter:

```
Blackbox/configure> system licenses ?

NAME
  licenses - Configure feature upgrade licenses

SYNTAX
  licenses license_type <cr>

DESCRIPTION
  license_type        -- Specifies the type of feature upgrade license
    The parameter may have any of the following values:
        enable_1_port -- Enable  1 port
        enable_2_ports-- Enable  2 ports
        enable_3_ports-- Enable  3 ports
        enable_4_ports-- Enable  4 ports
        BGP4           -- BGP4 routing
        vpn_mgmt       -- Enable VPN Mgmt License
        firewall       -- Enable Firewall and VPN Mgmt License
        vpn_plus_firewall-- Enable Advance VPN and Firewall License
```

To install the advanced VPN and firewall license and use all the security features available in this release, enter:

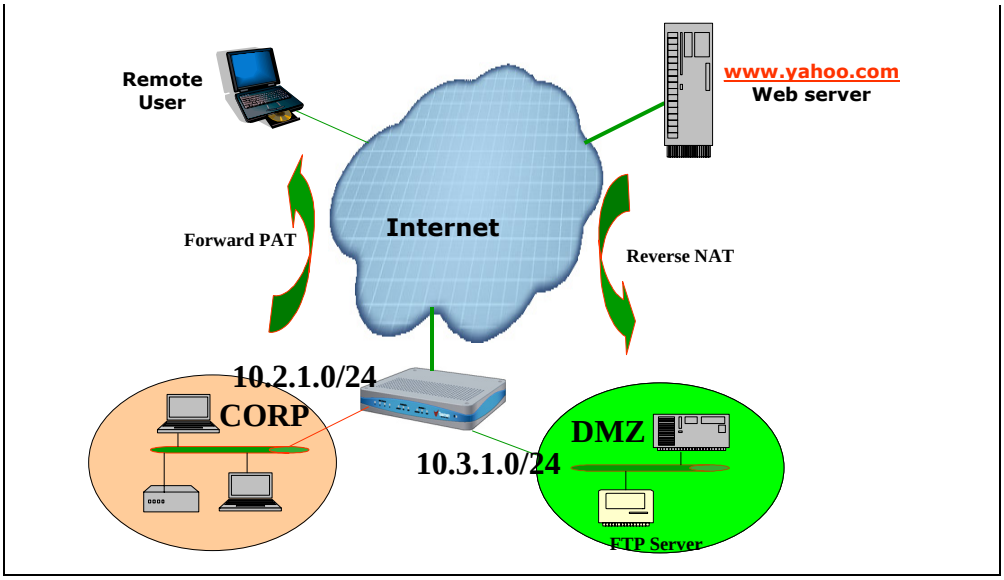
```
Blackbox/configure> system licenses vpn_plus_firewall
Enter Security Upgrade License key: 024f3bc296b4ea7265
```

10.2 Firewall Configuration Examples

10.2.1 Basic Firewall Configuration

Figure 18 illustrates the basic elements of a firewall. Refer to this illustration in the configuration example below.

Figure 18 Basic Firewall Configuration



A typical and basic firewall implementation is one which protects traffic to and from a network, a server farm, and the Internet. In this example, the firewall features in the Black Box router will protect the CORP network and the server farm in the DMZ from unauthorized access from the Internet.

To create this basic three-armed firewall configuration, complete these steps:

Step 1:Configure the Ethernet interfaces and the WAN interfaces with IP addresses:

```
Blackbox/configure> interface ethernet 0
Configuring existing Ethernet interface
Blackbox/configure/interface/ethernet 0> ip address 10.2.1.1 24
Blackbox/configure/interface/ethernet 0> exit
Blackbox/configure> interface ethernet 1
   Configuring existing Ethernet interface
Blackbox/configure/interface/ethernet 1> ip address 10.3.1.1 24
Blackbox/configure/interface/ethernet 1> exit
Blackbox/configure> interface bundle wan
Blackbox/configure/interface/bundle wan> link t1 1
Blackbox/configure/interface/bundle wan> encapsulation p
Blackbox/configure/interface/bundle wan> ip address 193.168.94.220 24
Blackbox/configure/interface/bundle wan> exit
```

Step 2: Create the security zones CORP and DMZ and attach interfaces:

```
Blackbox/configure> firewall corp
Blackbox/configure/firewall corp> interface ethernet0
Blackbox/configure/firewall corp> exit

Blackbox/configure> firewall dmz
Blackbox/configure/firewall dmz> interface ethernet1
Blackbox/configure/firewall dmz> exit

Blackbox/configure> firewall internet
Blackbox/configure/firewall internet> interface wan
Blackbox/configure/firewall internet> exit 2
```

Step 3: Verify that the interfaces are attached to the security zones:

```
Blackbox/configure> show firewall interface all

Interface      Map Name
---------      --------
ethernet0      corp
ethernet1      dmz
wan            internet
```

Step 4: Create policies for Security Zone CORP that:

- Allow all outgoing traffic (with firewall policy priority 1024)
- Deny all incoming traffic (with firewall policy priority 1021)
- Create an object of type **http-filter** to block java traffic
- Modify policy 1024 to pat all outgoing traffic using public IP 193.168.94.220
- Modify policy 1024 to add a java HTTP filter.

```
Blackbox/configure>
Blackbox/configure/firewall corp>
Blackbox/configure/firewall corp>
Blackbox/configure/firewall corp> policy 1024 out
Blackbox/configure/firewall corp/policy 1024 out> exit
Blackbox/configure/firewall corp> policy 1021 in deny
Blackbox/configure/firewall corp/policy 1021 in> exit
Blackbox/configure/firewall corp> object
Blackbox/configure/firewall corp/object> http-filter javadeny deny
*.java
Blackbox/configure/firewall corp/object> exit
Blackbox/configure/firewall corp> policy 1024 out nat-ip
193.168.94.220
Blackbox/configure/firewall corp/policy 1024 out> apply-object
http-filter javadeny
Blackbox/configure/firewall corp/policy 1024 out> exit
```

Step 5: Verify the firewall policy for Security Zone CORP:

```
Blackbox/configure> show firewall policy corp
Advanced: S - Self Traffic, F - Ftp-Filter, H - Http-Filter,
          R - Rpc-Filter, N - Nat-Ip/Nat-Pool, L - Logging,
          E - Policy Enabled, M - Smtp-Filter

Pri  Dir Source Addr        Destination Addr   Sport Dport Proto Action Advanced
---  --- -----------        ----------------   ----------------- ------ --------
1021 in  any                any                any   any   any   DENY   E
1022 out any                any                any   any   any   PERMIT SE
1023 in  any                any                any   any   any   PERMIT SE
1024 out any                any                any   any   any   PERMIT HNE
```

Step 6: Verify that the HTTP filter object in Security Zone CORP is created as configured.

```
Blackbox/configure> show firewall object http-filter corp
Object Name     Action Log File Extensions
-----------     ------ --- ---------------
javadeny         deny   no  *.java
Blackbox/configure>
```

Step 7: Create policies for Security Zone DMZ that:

- Create an object of type **nat-pool** with private IP address of FTP server
- Create an object of type **ftp-filter** to deny **put** and **mkdir** commands
- Create a firewall policy to allow inbound traffic to FTP server public IP address (193.168.94.221) of priority 100
- Modify policy 100 to add NAT pool object to translate incoming traffic for FTP server from public IP to private IP.
- Modify policy 100 to add an FTP filter.

```
Blackbox/configure> firewall dmz
Blackbox/configure/firewall dmz> object
Blackbox/configure/firewall dmz/object> ftp-filter putdeny deny put
mkdir
Blackbox/configure/firewall dmz/object> nat-pool ftpsrvr static
10.3.1.100
Blackbox/configure/firewall dmz/object> exit
Blackbox/configure/firewall dmz> policy 100 in address any any
193.168.94.221 32
Blackbox/configure/firewall dmz/policy 100 in> apply-object nat-pool
ftpsrvr
Blackbox/configure/firewall dmz/policy 100 in> apply-object
ftp-filter putdeny
Blackbox/configure/firewall dmz/policy 100 in> exit
Blackbox/configure/firewall dmz> exit
```

Step 8:Verify the firewall policy for Security Zone DMZ

```
Blackbox/configure> show firewall policy dmz
Advanced: S - Self Traffic, F - Ftp-Filter, H - Http-Filter,
          R - Rpc-Filter, N - Nat-Ip/Nat-Pool, L - Logging,
          E - Policy Enabled, M - Smtp-Filter

Pri  Dir Source Addr        Destination Addr   Sport Dport Proto Action Advanced
---  --- -----------        ----------------   ----------------- ------ --------
100  in  any                193.168.94.221/32 any   any   any   PERMIT FNE
1022 out any                any                any   any   any   PERMIT SE
1023 in  any                any                any   any   any   PERMIT SE
1024 out any                any                any   any   any   PERMIT E
```

Step 9: Verify that the FTP filter objects for Security Zone DMZ are created as configured:

```
Blackbox/configure> show firewall object ftp-filter dmz
Object Name     Action Log Commands
-----------     ------ --- --------
putdeny         deny   no  put mkdir
Blackbox/configure>
```

Step 10: Create a default route out of the WAN

```
Blackbox/configure> ip route 0.0.0.0 0 wan
Blackbox/configure>
```

Step 11:Verify the system configuration by displaying the running configuration.

```
Blackbox/configure> show configuration running
Please wait... (up to a minute)


terminal
  exit terminal
qos
  exit qos
module  t1 1
    alarms
      thresholds
        exit thresholds
      exit alarms
    linemode
      exit linemode
    exit t1
module  t1 2
    alarms
      thresholds
        exit thresholds
      exit alarms
    linemode
      exit linemode
    exit t1
module  t1 3
    alarms
      thresholds
        exit thresholds
      exit alarms
    linemode
      exit linemode
    exit t1
module  t1 4
    alarms
      thresholds
        exit thresholds
      exit alarms
    linemode
      exit linemode
    exit t1
aaa
  tacacs
    retries 2
    time_out 5
    server_port 49
    exit tacacs
  radius
    exit radius
  exit aaa
interface  ethernet 0
    ip  address 10.2.1.1 255.255.255.0
    ip  multicast
        mode ospfrip2
        exit multicast
    mtu 4000
    icmp
      exit icmp
```

```
    qos
      exit qos
    vrrp_mode 0
    aaa
      exit aaa
    crypto trusted
    exit ethernet
interface  ethernet 1
    ip  address 10.3.1.1 255.255.255.0
    ip  multicast
        mode ospfrip2
        exit multicast
    mtu 4000
    icmp
      exit icmp
    qos
      exit qos
    vrrp_mode 0
    aaa
      exit aaa
    crypto trusted
    exit ethernet
interface  bundle wan
    link  t1 1
    encapsulation ppp
    ip  address 193.168.94.220 255.255.255.0
    ip  multicast ospfrip2
    red
      exit red
    icmp
      exit icmp
    qos
      exit qos
    aaa
      exit aaa
    crypto untrusted
    exit bundle
interface  console
    aaa
      exit aaa
    exit console
snmp
  system_id Black Box
  enable_trap
    exit enable_trap
  exit snmp
hostname Black Box
log utc
telnet_banner
  exit telnet_banner
event
  exit event
system  logging
    no console
    syslog
      host_ipaddr 193.168.94.35
      exit syslog
    exit logging
ip
  load_balance per_flow
```

```
  multicast
    exit multicast
  route 0.0.0.0 0.0.0.0 wan 1
  exit ip
policy  community_list
    exit community_list
crypto
  exit crypto
firewall global
  exit firewall
firewall internet
  interface wan
  policy 1024 out self
    exit policy
  exit firewall
firewall corp
  interface ethernet0
  object
    http-filter javadeny deny *.java
    exit object
  policy 1021 in deny
    exit policy
  policy 1022 out self
    exit policy
  policy 1023 in self
    exit policy
  policy 1024 out nat-ip 193.168.94.220
    apply-object http-filter javadeny
    exit policy
  exit firewall
firewall dmz
  interface ethernet1
  object
    nat-pool ftpsrvr static 10.3.1.100 10.3.1.100
    ftp-filter putdeny deny put mkdir
    exit object
  policy 100 in address any any 193.168.94.221 32
    apply-object ftp-filter putdeny
    apply-object nat-pool ftpsrvr
    exit policy
  policy 1022 out self
    exit policy
  policy 1023 in self
    exit policy
  policy 1024 out
    exit policy
  exit firewall
Blackbox/configure>
```

10.2.1 Stopping DoS Attacks

The following commands show how to configure the firewall to defend against Denial of Service (DoS) attacks. Black Box provides protection against FTP bounce, ICMP error checks, IP sequence number checks, unaligned timestamps, MIME flooding, source routing checks, SYN flooding, and WIN nuke attacks. To configure the firewall for protection against all of these attacks, enter:

```
Blackbox> config term
Blackbox/configure> firewall global
Blackbox/configure/firewall global> dos-protect
Blackbox/configure/firewall global/dos-protect> enable-all
Blackbox/configure/firewall global/dos-protect> exit 2
Blackbox/configure>
```

10.2.2 Packet Reassembly

To configure the firewall to perform IP reassembly of oversized packets that have been fragmented, enter:

```
Blackbox> config term
Blackbox/configure> firewall global
Blackbox/configure/firewall global> ip-reassembly
Blackbox/configure/firewall global/ip-reassembly> fragment-count
100
Blackbox/configure/firewall global/ip-reassembly> fragment-size
56
Blackbox/configure/firewall global/ip-reassembly> packet-size
2048
Blackbox/configure/firewall global/ip-reassembly> timeout 20
```

10.3 NAT Configurations

Network Address Translation (NAT) was defined to serve two purposes:

- Allowed LAN administrators to create secure, private, non-routable IP networks behind firewalls
- Stretched the number of available IP addresses by allowing LANs to use one public (real) IP address as the gateway with a very large pool of NAT addresses behind it.

In the most common NAT application (which is to provide secure networking behind a firewall), the device (Black Box system) that connects the user LAN to the Internet will have two IP addresses:

- A private IP address on the LAN side for the RFC 1918 address range
- A public address, routable over the Internet, on the WAN side

Consider a PC on the LAN sending a packet destined for *some.server.com*. The source IP address and port are in the packet together with the destination IP address and port. When the packet arrives at the Black Box system it will be de-encapsulated, modified, and re-encapsulated. The re-encapsulated packet sent by the Black Box system destined for the Internet contains the Black Box system's public IP address, a source port allocated from its list of available ports, and the same destination IP address and port number generated by the PC. The Black Box system also adds an entry into a table it keeps, which maps the internal address and source port number that the PC generated against the port number it allocated to this session. Therefore, when *some.server.com* sends a reply packet to the PC, the Black Box system can quickly determine how it needs to re-write the packet before transmitting it back on to the LAN.

Dynamic NAT is used when packets destined for the Internet are transported from a LAN using the public source IP address assigned to the local router. Dynamic NAT performs this task well, but it does not permit providing services to the Internet from inside a LAN which requires the use of static NAT. Static NAT also requires a public address from the upstream service provider. Individual PCs within a LAN are assigned RFC 1918 reserved IP addresses to enable access to other PCs within the LAN. The Black Box system is configured with static mapping, which maps the internal RFC 1918 IP addresses for each PC to the appropriate public IP address. When traffic is sent to the public address listed in the static mapping, the Black Box system forwards the packets to the correct PC within the LAN, according to the mapping relationship established.

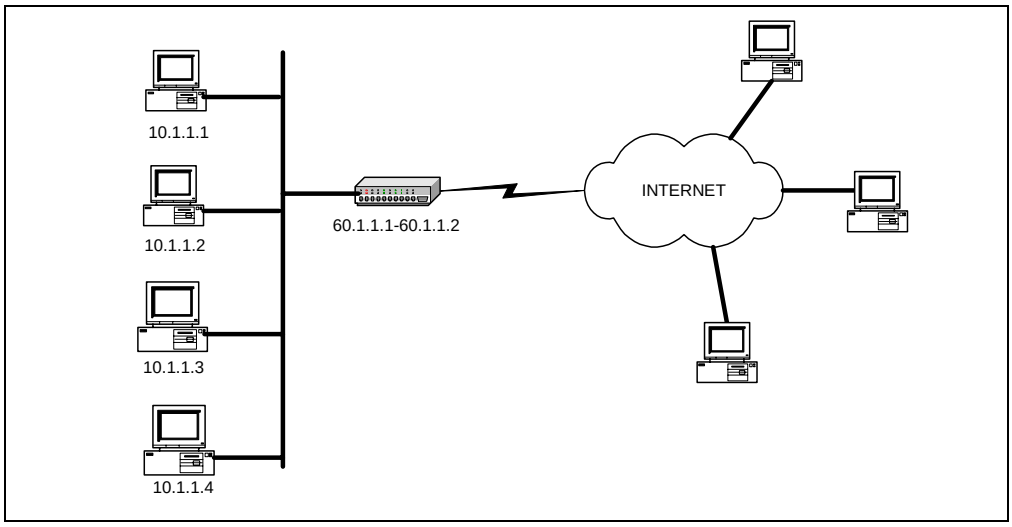
10.4 NAT Configuration Examples

10.4.1 Dynamic NAT (many to many)

In dynamic (many-to-many) NAT type, multiple source IP addresses in the corporate network will be mapped to multiple NAT IP addresses (not necessarily of equal number). For a set of local IP address from 10.1.1.1 to 10.1.1.4 there will be a set of NAT IP address from 60.1.1.1 to 60.1.1.2. In case of many-to-many NAT, only IP address translation takes place, i.e., if a packet travels from 10.1.1.1 to yahoo.com, Black Box-Firewall only substitutes the source address in the IP header with one of the NAT IP address and the source port will be the same as the original. If traffic emanates from the same client to any other server, the same NAT IP address is assigned. The advantage is that the NAT IP addresses are utilized in a better and optimum manner dynamically.

If a NAT IP address cannot be allocated dynamically at the connection creation time, the packet would be dropped.

Figure 19 Dynamic NAT



The dynamic NAT configuration shown in Figure 19 includes:

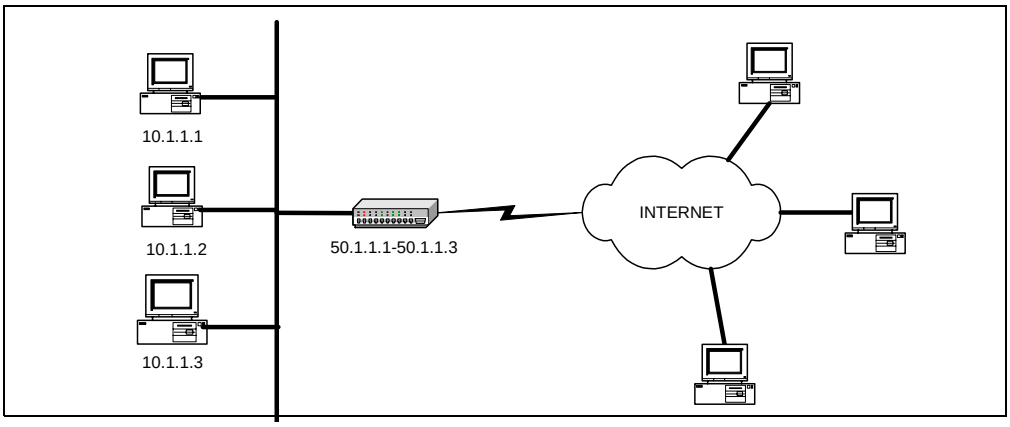
- Private network addresses:10.1.1.1—10.1.1.4
- Public (NAT) IP address range: 60.1.1.1—60.1.1.2

To create NAT pool with type **dynamic,** specify the IP address and the NAT ending IP address.Then add a policy with the source IP address range, and attach the NAT pool to the policy.

```
Blackbox/configure> firewall corp
Blackbox/configure/firewall corp> object
Blackbox/configure/firewall corp/object> nat-pool addresspoolDyna
dynamic 60.1.1.1 60.1.1.2
Blackbox/configure/firewall corp/object> exit
Blackbox/configure/firewall corp> policy 8 out address 10.1.1.1
10.1.1.4 any any
Blackbox/configure/firewall corp/policy 8 out> apply-object
nat-pool addresspoolDyna
Blackbox/configure/firewall corp/policy 8 out> exit 2
Blackbox/configure>
```

10.4.2 Static NAT (one to one)

Figure 20 Static NAT



In static (one-to-one) NAT type, for each IP address in the corporate network, one NAT IP address will be used. For example, for the three IP addresses from 10.1.1.1 to 10.1.1.3, there is a set of three NAT IP address from 50.1.1.1 to 50.1.1.3. In case of one-to-one NAT, only IP address translation takes place, that is, if a packet travels from 10.1.1.1 to yahoo.com, the Black Box-Firewall only substitutes the source address in the IP header with the NAT IP address. The source port will be the same as the original.

The static NAT configuration shown in Figure 20 includes:

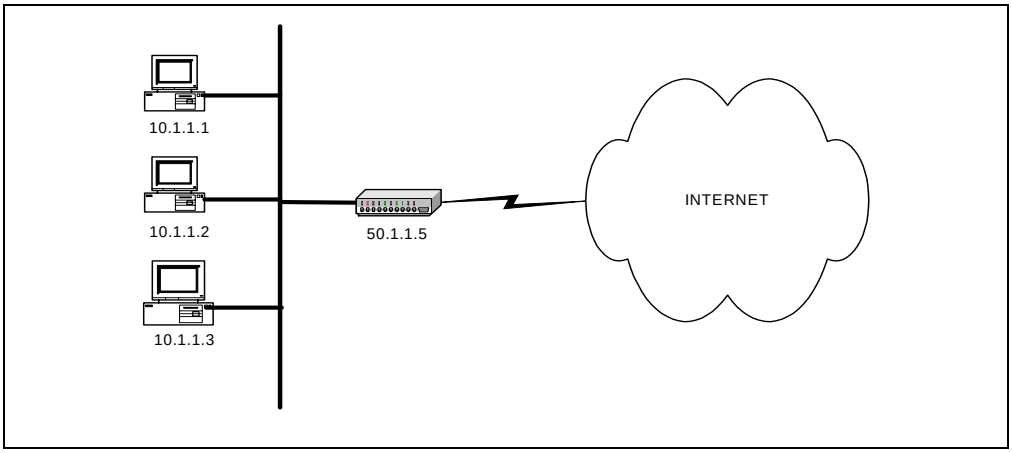
- Private network address:10.1.1.1—10.1.1.3
- Public (NAT) IP address range: 50.1.1.1—50.1.1.3

To create NAT pool with type **static**, specify the IP address and the ending NAT IP address. Add a policy with source IP address range and attach NAT pool to the policy.

```
Blackbox/configure> firewall corp
Blackbox/configure/firewall corp object
Blackbox/configure/firewall corp/object> nat-pool addresspoolStat
static 50.1.1.1 50.1.1.3
Blackbox/configure/firewall corp/object> exit
Blackbox/configure/firewall corp> policy 7 out address 10.1.1.1
10.1.1.3 any any
Blackbox/configure/firewall corp/policy 7 out> apply-object
nat-pool addresspoolStat
Blackbox/configure/firewall corp/policy 7 out> exit 2
Blackbox/configure>
```

10.4.3Port Address Translation (Many to one)

Figure 21 Mapping Multiple NAT Addresses to One Public IP Address



NAT allows multiple IP addresses to be mapped to one address.

There are two methods to configure Port Address Translation (PAT) on the Black Box gateway. In the first method, specify the IP address to the `nat-ip` parameter in the **`policy`** command. In the second method, create a pool of type PAT and then attach it to the policy.

In PAT, multiple hosts can share the same IP address.

The PAT configuration shown in Figure 21 includes:

- Private network address: 10.1.1.1—10.1.1.3
- PAT address: 50.1.1.5

Method:1 – Specifying NAT address with the policy command
To configure this method of PAT, add the policy with the source IP address range, then specify the `nat-ip` address in the **`policy`** command:

```
Blackbox/configure> firewall corp
Blackbox/configure/firewall corp> policy 2 out address 10.1.1.1
10.1.1.3 any any nat-ip 50.1.1.5
Blackbox/configure/firewall corp/policy 2 out> exit 2
Blackbox/configure>
```

Method:2 – Attaching nat pool to the policy
To configure the second type of NAT, create a NAT pool with type **`pat`** and specify the IP address. Then add the policy with the source IP address range. Finally, attach the NAT pool to the policy.

```
Blackbox/configure> firewall corp
Blackbox/configure/firewall corp> object
Blackbox/configure/firewall corp/object> nat-pool addresspoolPat
pat 50.1.1.5
Blackbox/configure/firewall corp/object> exit
Blackbox/configure/firewall corp> policy 2 out address 10.1.1.1
10.1.1.3 any any
Blackbox/configure/firewall corp/policy 2 out> apply-object
nat-pool addresspoolPat
Blackbox/configure/firewall corp/policy 2 out> exit 2
Blackbox/configure>
```

11
MULTIPATH MULTICAST CONFIGURATIONS

11.1Multipath Multicast

The multicast multipath feature allows load balancing on multicast traffic across equal cost paths. Equal cost multipath routing is useful when multiple equal cost routes to the same destination exist. These routes can be discovered and be used to provide load balancing among redundant paths. Commonly used methods for multipath forwarding are Round-Robin and Random. While these methods do provide a form of load balancing, but variable path MTUs, variable latencies, and debugging can limit the effectiveness of these methods.

The following methods have been developed to deal with the load balancing limitations of the Round-Robin and Random methods:

- **Modulo-N Hash** —To select a next-hop from the list of N next-hops, the router performs a modulo-N hash over the packet header fields that identify a flow."
- **Hash-Threshold**—The router first selects a key by performing a hash over the packet header fields that identify the flow. The N next-hops have been assigned unique regions in the hash functions output space. By comparing the hash value against region boundaries the router can determine which region the hash value belongs to and thus which next-hop to use.
- **Highest Random Weight (HRW)**—The router computes a key for each next-hop by performing a hash over the packet header fields that identify the flow, as well as over the address of the next-hop. The router then chooses the next-hop with the highest resulting key value.

The Round-Robin and Random methods are disruptive by design (that is, if there is no change to the set of next-hops, the path a flow takes changes every time). Modulo-N, Hash Threshold, and HRW are not disruptive.

RFC 2991 recommends to use HRW method to select the next-hop for multicast packet forwarding. or this reason, Black Box-only scenarios apply the HRW method as the default. This is similar to the Cisco Systems IPv6 multicast multipath implementation.

11.2Multipath Commands

The following table lists the multipath commands:

Task	Command
Enabling HRW method	Blackbox/configure/ip/multicast> multipath
Enabling Cisco method	Blackbox/configure/ip/multicast> multipath cisco
Disabling Multipath	Blackbox/configure/ip/multicast> no multipath Blackbox/configure/ip/multicast> no multipath cisco
Display RPF selection	Blackbox>show ip rpf <addr> <addr> - source or RP address

When multipath is disabled, Black Box selects the nexthop address with lowest ip address. For equal cost routes the nexthops are stored in the increasing (ascending) order of IP address. **show ip rpf** command displays the selected path, based on the configured multipath method and the nexthops of the best route to the IP address passed.

11.2.1 Multipath Examples

The following examples illustrate how the multicast commands are used:

The following command enables compatibility between the Black Box router and equipment running Cisco IOS.

```
Blackbox/configure/ip/multicast> multipath mode cisco
Blackbox/configure/ip/multicast>
```

The following command enables HRW compatibility.

```
Blackbox/configure/ip/multicast> multipath
Blackbox/configure/ip/multicast>
```

The following example shows how to see the reverse path forwarding information for the RP at 201.1.1.99:

```
Blackbox> show ip rpf 201.1.1.99
```

12
CONFIGURING NAT

12.1Network Address Translation

Network Address Translation (RFC 1631) is commonly known as NAT. This application discusses NAT and provides a technical explanation and configuration examples.

Features:

- Dynamic Address/Port Translation
- Static Address/Port Translation
- Forward and Reverse NAT
- Non-Translated Address Pass Through

In the most common NAT application, the device (Black Box system) that connects the user LAN to the Internet will have two IP addresses:

- A private IP address on the LAN side for the RFC 1918 address range
- A public address, routable over the Internet, on the WAN side

Consider a PC on the LAN sending a packet destined for some.server.com. The source IP address and port are in the packet together with the destination IP address and port. When the packet arrives at the Black Box system it will be de-encapsulated, modified, and re-encapsulated. The re-encapsulated packet sent by the Black Box system destined for the Internet contains the Black Box system's public IP address, a source port allocated from its list of available ports, and the same destination IP address and port number generated by the PC. The Black Box system also adds an entry into a table it keeps, which maps the internal address and source port number that the PC generated against the port number it allocated to this session. Therefore, when some.server.com sends a reply packet to the PC, the Black Box system can quickly determine how it needs to re-write the packet before transmitting it back on to the LAN.

12.1.1 Dynamic NAT

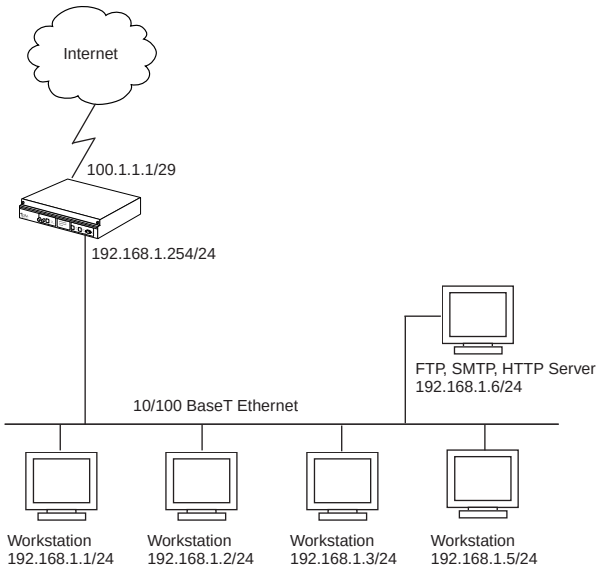
Dynamic NAT is used when packets destined for the Internet are transported from a LAN using the public source IP address assigned to the local router. Dynamic NAT performs this task well, but it does not permit providing services to the Internet from inside a LAN. In these instances, static NAT is used.

12.1.2 Static NAT

Static NAT also requires a public address from the upstream service provider. Individual PCs within a LAN are assigned RFC 1918 reserved IP addresses to enable access to other PCs within the LAN. The Black Box system is configured with static mapping, which maps the internal RFC 1918 IP addresses for each PC to the appropriate public IP address. Then when traffic is sent to the public address listed in the static mapping, the Black Box system forwards the packets to the correct PC within the LAN, according to the mapping relationship established.

Figure 22 illustrates dynamic and static NAT. The static translation between 192.168.1.6 and 100.1.1.6 automatically matches the port addresses, thus a request destined for 100.1.1.6 tcp port 25 is translated to 192.168.1.6 tcp port 25 and so on.

Figure 22 Dynamic and Static NAT

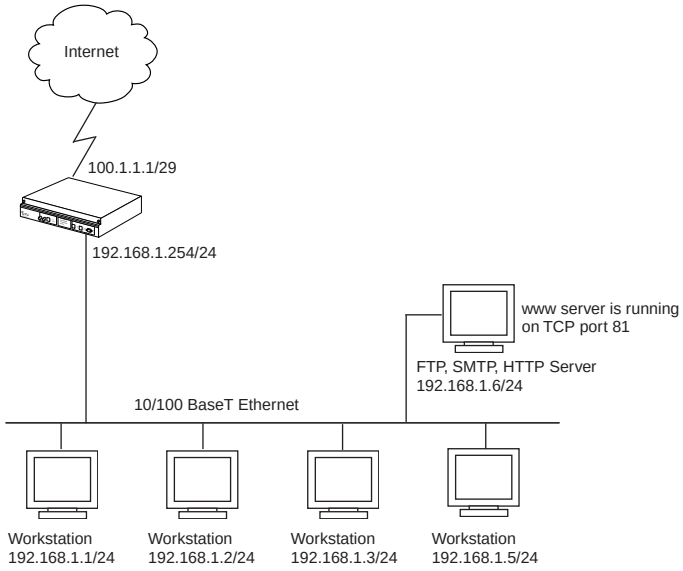


12.1.3 Configuration for Figure 1

```
Blackbox> configure terminal
Blackbox/configure> interface bundle Trenton
Blackbox/configure/interface/bundle Trenton> nat
Blackbox/configure/interface/bundle Trenton/nat> enable dynamic
Blackbox/configure/interface/bundle Trenton/nat> enable static
Blackbox/configure/interface/bundle Trenton/nat> address 192.168.1.6 100.1.1.6
```

Figure 23 provides an example of static port mapping. TCP port 81 of the web server at private address 192.168.1.6 is mapped to the same TCP port of the public address.

Figure 23 Mapping Ports



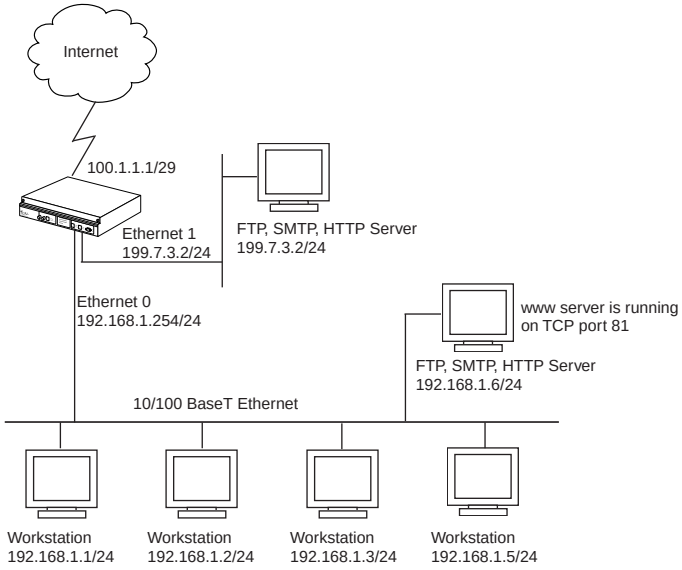
12.1.4 Configuration for Figure 2

```
Blackbox> configure terminal
Blackbox/configure> interface bundle Trenton
Blackbox/configure/interface/bundle Trenton> nat
Blackbox/configure/interface/bundle Trenton/nat> enable dynamic
Blackbox/configure/interface/bundle Trenton/nat> enable static
Blackbox/configure/interface/bundle Trenton/nat> address 192.168.1.6 81 100.1.1.6 81
```

12.1.5 Reverse NAT

Reverse NAT could be used in a situation where one LAN is using private RFC 1918 IP addresses and a second LAN is using “real” Internet routable IP addresses. Figure 24 illustrates how reverse NAT would be applied.

Figure 24 Reverse NAT



12.1.6 Configuration for Figure 3

```
Blackbox> configure terminal
Blackbox/configure> interface ethernet 0
Blackbox/configure/interface/ethernet0> nat
Blackbox/configure/interface/ethernet0/nat> reverse
Blackbox/configure/interface/ethernet0/nat> ip 100.1.1.1
Blackbox/configure/interface/ethernet0/nat> enable dynamic
Blackbox/configure/interface/ethernet0/nat> enable static
Blackbox/configure/interface/ethernet0/nat> port tcp 100.1.1.6 25 192.168.1.6 25
Blackbox/configure/interface/ethernet0/nat> port tcp 100.1.1.6 81 192.168.1.6 81
Blackbox/configure/interface/ethernet0/nat> port tcp 100.1.1.6 21 192.168.1.6 21
```

13
NAT CONFIGURATION EXAMPLES

13.1 NAT Configurations

Network Address Translation (NAT) was defined to serve two purposes:

- Allowed LAN administrators to create secure, private, non-routable IP networks behind firewalls
- Stretched the number of available IP addresses by allowing LANs to use one public (real) IP address as the gateway with a very large pool of NAT addresses behind it.

In the most common NAT application (which is to provide secure networking behind a firewall), the device (Black Box system) that connects the user LAN to the Internet will have two IP addresses:

- A private IP address on the LAN side for the RFC 1918 address range
- A public address, routable over the Internet, on the WAN side

Consider a PC on the LAN sending a packet destined for *some.server.com*. The source IP address and port are in the packet together with the destination IP address and port. When the packet arrives at the Black Box system it will be de-encapsulated, modified, and re-encapsulated. The re-encapsulated packet sent by the Black Box system destined for the Internet contains the Black Box system's public IP address, a source port allocated from its list of available ports, and the same destination IP address and port number generated by the PC. The Black Box system also adds an entry into a table it keeps, which maps the internal address and source port number that the PC generated against the port number it allocated to this session. Therefore, when *some.server.com* sends a reply packet to the PC, the Black Box system can quickly determine how it needs to re-write the packet before transmitting it back on to the LAN.

Dynamic NAT is used when packets destined for the Internet are transported from a LAN using the public source IP address assigned to the local router. Dynamic NAT performs this task well, but it does not permit providing services to the Internet from inside a LAN which requires the use of static NAT. Static NAT also requires a public address from the upstream service provider. Individual PCs within a LAN are assigned RFC 1918 reserved IP addresses to enable access to other PCs within the LAN. The Black Box system is configured with static mapping, which maps the internal RFC 1918 IP addresses for each PC to the appropriate public IP address. When traffic is sent to the public address listed in the static mapping, the Black Box system forwards the packets to the correct PC within the LAN, according to the mapping relationship established.

13.1 NAT Configuration Examples

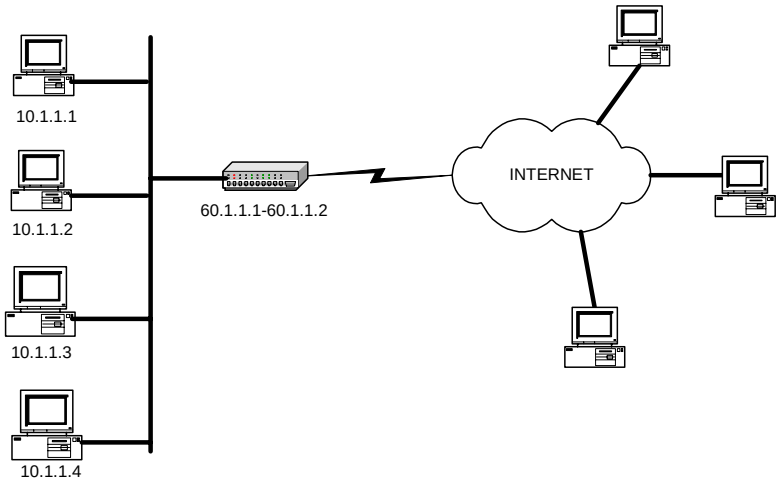
13.1.1Dynamic NAT (many to many)

In dynamic (many-to-many) NAT type, multiple source IP addresses in the corporate network will be mapped to multiple NAT IP addresses (not necessarily of equal number). For a set of local IP address from 10.1.1.1 to 10.1.1.4 there will be a set of NAT IP address from 60.1.1.1 to 60.1.1.2. In case of many-to-many NAT, only IP address

translation takes place, i.e., if a packet travels from 10.1.1.1 to yahoo.com, Black Box-Firewall only substitutes the source address in the IP header with one of the NAT IP address and the source port will be the same as the original. If traffic emanates from the same client to any other server, the same NAT IP address is assigned. The advantage is that the NAT IP addresses are utilized in a better and optimum manner dynamically.

If a NAT IP address cannot be allocated dynamically at the connection creation time, the packet would be dropped.

Figure 25 Dynamic NAT



The dynamic NAT configuration shown in Figure 25 includes:

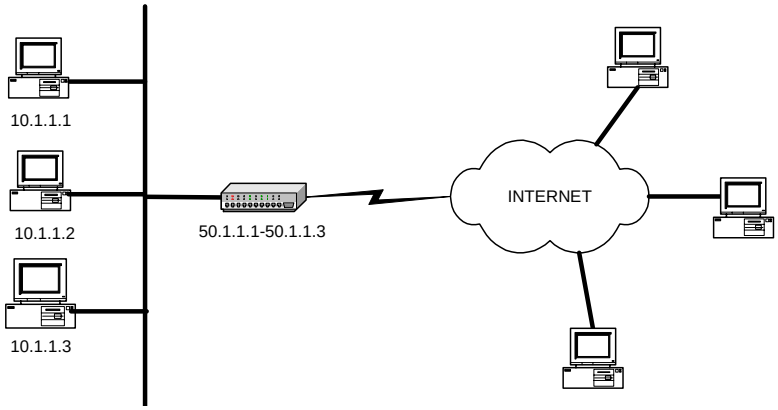
- Private network addresses:10.1.1.1—10.1.1.4
- Public (NAT) IP address range: 60.1.1.1—60.1.1.2

To create NAT pool with type **dynamic,** specify the IP address and the NAT ending IP address.Then add a policy with the source IP address range, and attach the NAT pool to the policy.

```
Blackbox/configure> firewall corp
Blackbox/configure/firewall corp> object
Blackbox/configure/firewall corp/object> nat-pool addresspoolDyna dynamic
60.1.1.1 60.1.1.2
Blackbox/configure/firewall corp/object> exit
Blackbox/configure/firewall corp> policy 8 out address 10.1.1.1 10.1.1.4 any any
Blackbox/configure/firewall corp/policy 8 out> apply-object nat-pool
addresspoolDyna
Blackbox/configure/firewall corp/policy 8 out> exit 2
Blackbox/configure>
```

13.1.2Static NAT (one to one)

Figure 26 Static NAT



In static (one-to-one) NAT type, for each IP address in the corporate network, one NAT IP address will be used. For example, for the three IP addresses from 10.1.1.1 to 10.1.1.3, there is a set of three NAT IP address from 50.1.1.1 to 50.1.1.3. In case of one-to-one NAT, only IP address translation takes place, that is, if a packet travels from 10.1.1.1 to yahoo.com, the Black Box-Firewall only substitutes the source address in the IP header with the NAT IP address. The source port will be the same as the original.

The static NAT configuration shown in Figure 26 includes:

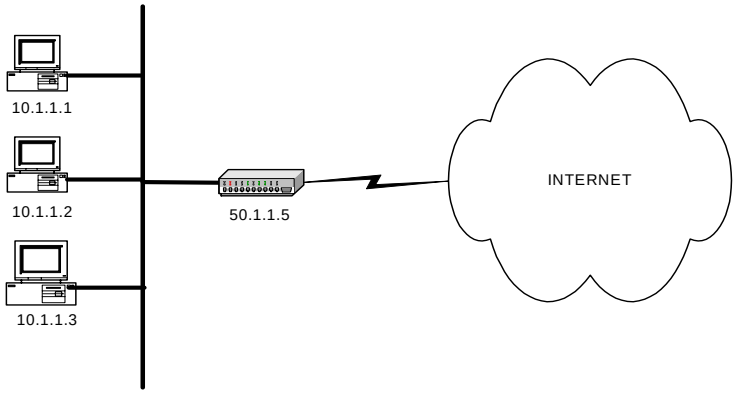
- Private network address:10.1.1.1—10.1.1.3
- Public (NAT) IP address range: 50.1.1.1—50.1.1.3

To create NAT pool with type **static**, specify the IP address and the ending NAT IP address. Add a policy with source IP address range and attach NAT pool to the policy.

```
Blackbox/configure> firewall corp
Blackbox/configure/firewall corp object
Blackbox/configure/firewall corp/object> nat-pool addresspoolStat static 50.1.1.1
50.1.1.3
Blackbox/configure/firewall corp/object> exit
Blackbox/configure/firewall corp> policy 7 out address 10.1.1.1 10.1.1.3 any any
Blackbox/configure/firewall corp/policy 7 out> apply-object nat-pool addresspoolStat
Blackbox/configure/firewall corp/policy 7 out> exit 2
Blackbox/configure>
```

13.1.3Port Address Translation (Many to one)

Figure 27 Mapping Multiple NAT Addresses to One Public IP Address



NAT allows multiple IP addresses to be mapped to one address.

There are two methods to configure Port Address Translation (PAT) on the Black Box gateway. In the first method, specify the IP address to the `nat-ip` parameter in the **`policy`** command. In the second method, create a pool of type PAT and then attach it to the policy.

In PAT, multiple hosts can share the same IP address.

The PAT configuration shown in Figure 27 includes:

- Private network address: 10.1.1.1—10.1.1.3
- PAT address: 50.1.1.5

Method:1 – Specifying NAT address with the policy command

To configure this method of PAT, add the policy with the source IP address range, then specify the `nat-ip` address in the **`policy`** command.

```
Blackbox/configure> firewall corp
Blackbox/configure/firewall corp> policy 2 out address 10.1.1.1 10.1.1.3 any any nat-ip
50.1.1.5
Blackbox/configure/firewall corp/policy 2 out> exit 2
Blackbox/configure>
```

Method:2 – Attaching nat pool to the policy

To configure the second type of NAT, create a NAT pool with type **`pat`** and specify the IP address. Then add the policy with the source IP address range. Finally, attach the NAT pool to the policy.

```
Blackbox/configure> firewall corp
Blackbox/configure/firewall corp> object
Blackbox/configure/firewall corp/object> nat-pool addresspoolPat pat 50.1.1.5
Blackbox/configure/firewall corp/object> exit
Blackbox/configure/firewall corp> policy 2 out address 10.1.1.1 10.1.1.3 any any
Blackbox/configure/firewall corp/policy 2 out> apply-object nat-pool addresspoolPat
Blackbox/configure/firewall corp/policy 2 out> exit 2
Blackbox/configure>
```

14
REMOTE ACCESS VPNS

14.1 Secure Remote Access Using IPSec VPN

The corporate network no longer has a clearly defined perimeter inside secure building and locked equipment closets. Increasingly, companies have a need to provide remote access to their corporate resources for the employees on the move.

Traditionally, remote users could access the corporate LAN through dial-up and ISDN lines which were terminated in the corporate remote access servers. However, these point-to-point connection technologies do not scale well to the growing number of remote users and the corresponding increase in the infrastructure investments and maintenance costs.

A solution to meeting the needs of increasing numbers of remote users and for controlling access costs is to provide remote access through the Internet using firewalls and a Virtual Private Network (VPN). Internet Protocol Security (IPSec) keeps the connection safe from unauthorized users.

In a typical IPSec remote access scenario, the mobile user has connectivity to Internet and an IPSec VPN client loaded on their PC. The remote user connects to the Internet through their Internet service provider and then initiates a VPN connection to the IPSec security gateway (the VPN server) of the corporate office, which is typically an always-on Internet connection.

One of the main limitations in providing remote access is the typical remote user connects with a dynamically assigned IP address provided by the ISP. IPSec uses the IP address of users as an index to apply the Internet Key Exchange (IKE) and IPSec policies to be used for negotiation with each peer. When the VPN client has a dynamic IP address, the VPN server cannot access the policies based on the IP address of the client. Instead, the VPN server uses the identity of the VPN client to access the policies.

14.2 Access Methods

Black Box supports two types of IPSec remote access using VPNs.

14.2.1 Remote Access: User Group

One of the methods to achieve IPSec remote access in Black Box is the user group method. In this method, the administrator creates an IKE policy for a logical group of users such as a department in an organization. Each user in the group is identified with unique information that is uniquely configured in the IKE policy. Also, an IPSec template is attached to the user group.

Once the VPN user is authenticated using IKE, the users dynamically-assigned IP address is added to the destination address field in the IPSec template attached to the user group. The VPN user now has the required IPSec policy that allows access through the gateway to the corporate LAN.

14.2.2 Remote Access: Mode Configuration

The other method to achieve IPSec remote access in Black Box is the mode configuration method.

This method makes the VPN client an extension of the LAN being accessed by the VPN client. The remote client appears as a network accessing some resource behind the VPN server.

The VPN client is allocated a private IP address by the VPN server and the client uses this as the source IP address in the inner IP header in tunnel mode.

In tunnel mode, at each IKE end point, the IP traffic to be protected is completely encapsulated with another IP packet. In this, the inner IP header remains the same as seen in the original traffic to be protected. In the outer IP header, the source and destination addresses are the addresses of the tunnel end points.

Typically, for a remote user, the source address of the outer IP header is the dynamic public IP address provided by the ISP. When mode configuration is enabled, the source address of the inner IP header is the private address allocated by the VPN server to the VPN client.

As in the case of user group method, the administrator creates an IKE policy for a logical group of users such as a department in an organization. The identity information used to identify each user uniquely is configured in the IKE policy. The IKE policy is attached to a mode configuration record. The mode configuration record contains an IPSec policy template to be used for creating dynamic IPSec policy. Also, the record contains one or more pools of private IP addresses to be used for allocating the addresses to the VPN clients. Besides the private IP address, the VPN server can also provide WINS and DNS server addresses.

Upon successful IKE authentication of a VPN client, the server checks whether the IKE policy used to authenticate the VPN client is enabled for mode configuration. If so, the server allocates a private IP address from one of the IP pools in the mode configuration record to the VPN client. The destination address field in the IPSec template attached to the user group is filled in with the private IP address allocated to the VPN client and this is installed as an IPSec policy.

14.3 Configuration Examples

The following examples illustrate configurations for creating secure remote VPN access to:

- An individual SNMP user managing the gateway (user group method)
- The corporate LAN for multiple users (mode configuration method)

14.4 IPSec Remote Access User Group Method – Single Proposal, Pre-shared Key Authentication

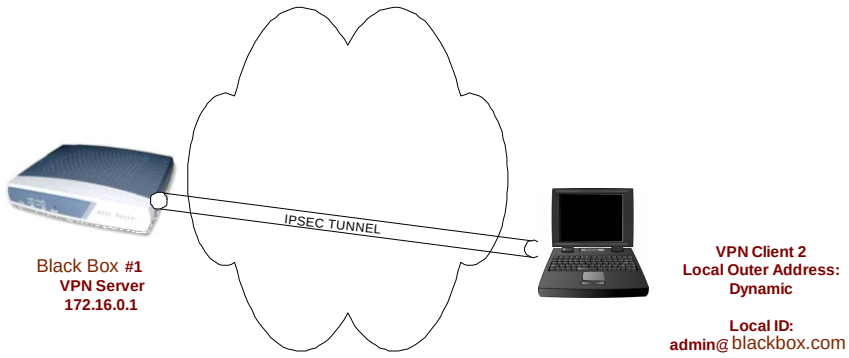
The following example demonstrates how to manage the Black Box gateway from a secure VPN management host. An application would look like a host in a remote site is interested in managing Black Box router using SNMP. But the remote host is interested in doing securely. The SNMP response that is generated in Black Box router for a request from the management host is called self-generated traffic.

The Black Box gateway provides a map called **Self** for self-generated traffic. This map is created automatically when the gateway comes up.

The security requirements for the management tunnel are:

- 3DES with SHA1,Pre-shared key authentication, XAuth
- IPSec ESP with AES128 and HMAC-SHA1

Figure 28 User Group Remote Access Configuration



To create the user group configuration enter:

```
Blackbox>configure term
Blackbox/configure>interface bundle wan
Blackbox/configure/interface/bundle wan>link t1 1-2
Blackbox/configure/interface/bundle wan>ip address 172.16.0.1 32[1]
Blackbox/configure/interface/bundle wan>crypto internet
```

To configure the IKE policy for negotiating with the remote VPN client needing access (note that the IKE and IPSec policies for management (self) tunnel need to be defined in the “Self” map):

```
Blackbox/configure>crypto Self
Blackbox/configure/crypto>dynamic
Blackbox/configure/crypto/dynamic>ike policy admin user-group
Blackbox/configure/crypto/dynamic/ike/policy admin>local-address 172.16.0.1
Blackbox/configure/crypto/dynamic/ike/policy admin>remote-id email-id sampledata Black Boxuser
Blackbox/configure/crypto/dynamic/ike/policy admin>key pskforadminuser
Blackbox/configure/crypto/dynamic/ike/policy admin>proposal 1
Blackbox/configure/crypto/dynamic/ike/policy admin/proposal 1>encryption-algorithm 3des-cbc
Blackbox/configure/crypto/dynamic/ike/policy admin/proposal 1>client authentication radius
```

To configure the IPSec policy for negotiating with VPN client needing access to the security gateway.

```
Blackbox/configure/crypto/dynamic>ipsec policy admin user-group
Blackbox/configure/crypto/dynamic/ipsec/policy admin>match address 172.16.0.1 32
Blackbox/configure/crypto/dynamic/ipsec/policy admin> proposal 1
Blackbox/configure/crypto/dynamic/ipsec/policy admin/proposal 1>encryption-algorithm aes128-cbc
```

1. error message saying Bundle is not yet encapped.

14.5 IPSec Remote Access Mode Configuration Group Method

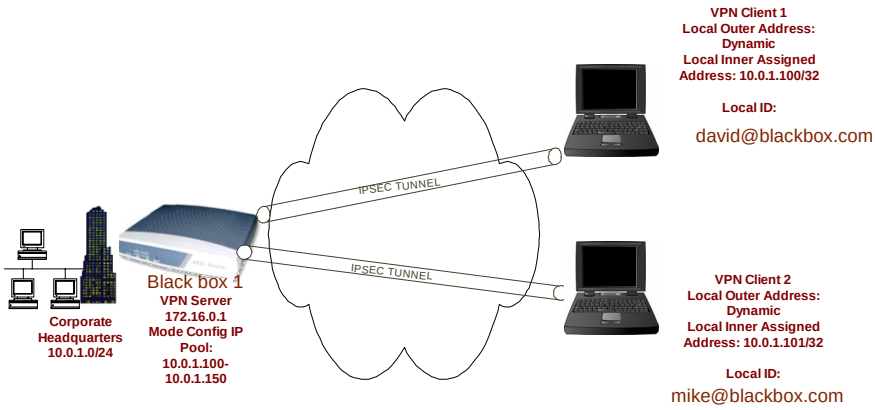
The following example demonstrates how to configure a Black Box router to be an IPSec VPN server using mode-configuration method. The client could be any standard mode config enabled IPSec VPN client.

In this example, the client needs to access the corporate private network 10.0.1.0/24 through the VPN tunnel. The server has a pool of IP addresses from 20.1.1.100 through 20.1.1.150 to be allocated for mode config enabled VPN clients. The assigned IP address is used by the VPN client as the source address in the inner IP header. The outer IP header will carry the dynamic IP address assigned by the Internet Service Provider as the source address. The security requirements are as follows:

3DES with SHA1, Mode Config

IPSec ESP tunnel with AES256 and HMAC-SHA1

Figure 29 Configuration Mode Remote Access Configuration



To configure the VPN gateway:

```
Blackbox>configure term
Blackbox/configure>interface ethernet 1
Blackbox/configure/interface/ethernet 1>ip address 10.0.1.1 24
Blackbox/configure/interface/ethernet 1>crypto corp

Blackbox/configure> interface bundle wan
Blackbox/configure/interface/bundle wan>link t1 1-2
Blackbox/configure/interface/bundle wan>ip address 172.16.0.1 32[1]
Blackbox/configure/interface/bundle wan>crypto internet
```

To configure the IKE policy for negotiating with VPN clients needing access to the corporate private network 10.0.1.0.

```
Blackbox/configure>crypto corp
Blackbox/configure/crypto>dynamic
Blackbox/configure/crypto/dynamic>ike policy IDCsales modecfg-group
Blackbox/configure/crypto/dynamic/ike/policy IDCsales>modeconfig-group
Blackbox/configure/crypto/dynamic/ike/policy IDCsales>local-address 172.16.0.1
To configure the user name (optional) for remote-id:
Blackbox/configure/crypto/dynamic/ike/policy IDCsales>remote-id email-id sampledata
david@Blackbox.com
Blackbox/configure/crypto/dynamic/ike/policy IDCsales>remote-id email-id sampledata
mike@Blackbox.com
Blackbox/configure/crypto/dynamic/ike/policy IDCsales>key pskforsalesusers
Blackbox/configure/crypto/dynamic/ike/policy IDCsales>proposal 1
Blackbox/configure/crypto/dynamic/ike/policy IDCsales>encryption-algorithm 3des-cbc
Blackbox/configure/crypto/dynamic/ike/policy IDCsales>exit
Blackbox/configure/crypto/dynamic>client configuration
# configure address pool for modecfg client
address-pool 1 20.1.1.100 20.1.1.150
```

To configure the IPSec policy for negotiating with VPN clients needing access to the corporate private network 10.0.1.0.

```
Blackbox/configure/crypto/dynamic>ipsec policy IDCsales
Blackbox/configure/crypto/dynamic/ipsec/policy IDCSales>match address 10.0.1.0 24
Blackbox/configure/crypto/dynamic/ipsec/policy IDCSales>proposal 1
Blackbox/configure/crypto/dynamic/ipsec/policy IDCSales/proposal 1>encryption-algorithm
aes256-cbc
```

1. Bundle must be encapsulated first steps TBC.

15
NETWORKING WITH ROUTING INFORMATION PROTOCOL

15.1Routing Information Protocol

15.1.1Configuring RIP for Ethernet 0 and WAN 1 Interfaces

```
LR1114A> configure terminal
LR1114A/configure> router rip
LR1114A/configure/router rip> interface ethernet0
LR1114A/configure/router rip/interface ethernet0> exit
LR1114A/configure/router rip> interface wan1
LR1114A/configure/router rip> exit
```

15.1.2Displaying RIP Configuration

Execute **show ip rip global** to display RIP configuration information

Figure 30 show ip rip global Command

```
> show ip rip global
Router RIP is enabled
        Mode: RIP 2
        Distance: 100
        Default Metric: 1
        Timers:
                Update: 30 seconds
                Holddown: 120 seconds
                Flush: 180 seconds
```

15.1.3Displaying All Configured RIP Interfaces

Execute **show ip rip interface all** to display information about all configured RIP interfaces.

Figure 31 show ip rip interface all Command

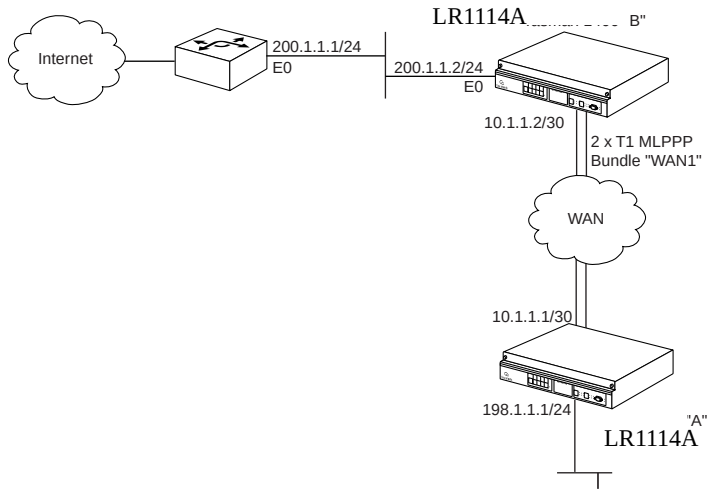
```
> show ip rip interface all
RIP is configured for interface <ethernet0>
        Mode: RIP 2
        Metric: 5
        Authentication: None
        Split Horizon: Poison
        Routers : None
        Interface state:  Broadcast Multicast Active
```

16
CONFIGURING STATIC ROUTES

16.1 Static Routing Configuration

All Black Box systems support IP routing utilizing static routes. The following diagram shows a remote Black Box “A” connected over an MLPPP bundle to the main Black Box “B”. Black Box B in turn routes to the customer router.

Figure 32 IP Routing



The customer router Ethernet 0 IP address is 200.1.1.1 255.255.255.0, and the IP route is 198.1.1.0 255.255.255.0 200.1.1.2 2.

16.1.1Configure the Router at Site “A”

```
Blackbox> configure term
Blackbox/configure> interface ethernet 0
Blackbox/configure/interface/ethernet> ip addr 198.1.1.1 255.255.255.0
Blackbox/configure/interface/ethernet> exit

Blackbox/configure> interface bundle wan1
Blackbox/configure/interface/bundle> link t1 1-2
Blackbox/configure/interface/bundle> encap ppp
Blackbox/configure/interface/bundle> ip addr 10.1.1.1 255.255.255.252
Blackbox/configure/interface/bundle> exit

Blackbox/configure> ip routing
Blackbox/configure> ip route 0.0.0.0 0.0.0.0 10.1.1.2 1
```

16.1.2Configure the Router at site “B”

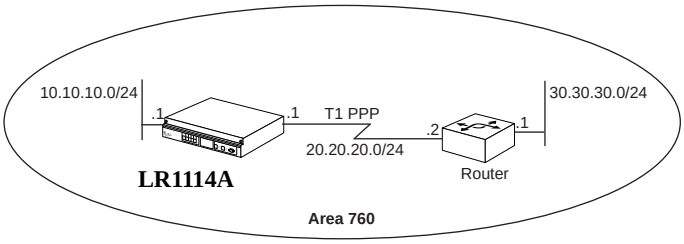
```
Blackbox> configure term
Blackbox/configure> interface ethernet 0
Blackbox/configure/interface/ethernet> ip addr 200.1.1.2 255.255.255.0
Blackbox/configure/interface/ethernet> exit

Blackbox/configure> interface bundle wan 1
Blackbox/configure/interface/bundle> link t1 1-2
Blackbox/configure/interface/bundle> encapp ppp
Blackbox/configure/interface/bundle> ip addr 10.1.1.2 255.255.255.252
Blackbox/configure/interface/bundle> exit

Blackbox/configure> ip routing
Blackbox/configure> ip route 198.1.1.0 255.255.255.0 10.1.1.1 1
Blackbox/configure> ip route 0.0.0.0 0.0.0.0 200.1.1.1 1
Blackbox/configure> exit
```

17
CONFIGURING OPEN SHORTEST PATH FIRST ROUTING

17.1 OSPF Routing Protocol

The following example shows a Black Box LR1114A connected to a router over a single T1 link. IP addresses 10.10.10.0, 20.20.20.0, and 30.30.30.0 are assigned to area 760.

Figure 33 Configuring OSPF Between a Black Box LR1114A System and a Router



17.1.1Configuring the host name

```
Blackbox> configure terminal
Blackbox/configure> hostname LR1114A
```

17.1.2Configuring interface ethernet 0

```
LR1114A/configure> interface ethernet 0
LR1114A/configure/interface/ethernet 0> ip address 10.10.10.1 24
LR1114A/configure/interface/ethernet 0> exit
```

17.1.3Configuring interface bundle Dallas

```
LR1114A/configure> interface bundle Dallas
LR1114A/configure/interface/bundle Dallas> link t1 1
LR1114A/configure/interface/bundle Dallas> encapsulation ppp
LR1114A/configure/interface/bundle Dallas> ip address 20.20.20.1 24
LR1114A/configure/interface/bundle Dallas> exit
```

17.1.4Configuring ospf

```
LR1114A/configure> router routerid 10.10.10.1
LR1114A/configure> router ospf
LR1114A/configure/router/ospf> area 760
LR1114A/configure/router/ospf/area 760> exit
```

17.1.5Configuring ospf interface parameters

```
LR1114A/configure/router/ospf> interface Dallas area_id 760
LR1114A/configure/router/ospf/interface Dallas> exit
LR1114A/configure/router/ospf> interface ethernet0 area_id 760
LR1114A/configure/router/ospf/interface ethernet0> exit 3
```

17.1.6Displaying neighbors

Note that “display” and “show” can be used interchangeably in the CLI tree hierarchy.

Execute **show ip ospf neighbor list** on the Black Box LR1114A to display the neighbor information. In this example, the state is in FULL adjacency with the router.

Figure 34 show ip ospf neighbor list Command

```
LR1114A> show ip ospf neighbor list

Neighbor ID   PRI  State     Dead Time  Address       Interface
-----------   ---  -----     ---------  -------       ---------
30.30.30.1     1    FULL/ -   00:00:30  20.20.20.2    TMan1
```

17.1.7Displaying ospf routes

Execute **show ip ospf routes** on the Black Box LR1114A to display the OSPF routes learned from neighbors. The following display shows the route 30.30.30.0/24, which was learned through OSPF from the router advertisements.

Figure 35 show ip ospf routes Command

```
LR1114A> show ip ospf routes

OSFP ROUTE TABLE

Codes: A - OSPF intra area   IA - OSPF inter area,
   E1 - OSPF external type 1, E2 - OSPF external type 2

Destination       Gateway     Interface Protocol  Type  Metric
Preference
-----------       -------     --------- --------  ----  ------
----------
```

The metric shows a value of 2. By default, Black Box assigns a cost value of 1 to all interfaces. The cost can be changed by entering it under the appropriate interface in the OSPF command tree structure. For example:

```
LR1114A/configure> router ospf
LR1114A/configure/router/ospf> interface Dallas area_id 760
LR1114A/configure/router/ospf/interface/Dallas> cost 10
LR1114A/configure/router/ospf/interface/Dallas> exit 3
```

This would change the cost of bundle link Dallas from default (1) to 10. If the interface is already configured, then entering **area_id 760** is optional.

17.1.8Displaying IP routes

Execute **show ip routes** to display all the active routes in the routing table.

18
CONFIGURING GENERIC ROUTING ENCAPSULATION

18.1 Configuring GRE

Generic Routing Encapsulation (GRE) is a standards-based (RFC1701, RFC2784) tunneling protocol that can encapsulate a wide variety of protocol packet types inside IP tunnels, creating a virtual point-to-point link between routers at remote points over an IP network. A tunnel is a logical interface that provides a way to encapsulate passenger packets inside a transport protocol. By connecting multiprotocol subnetworks in a single-protocol backbone environment, IP tunneling using GRE allows network expansion across a single-protocol backbone environment.

IPSec and GRE complement each other well, while IPSec provides a secure method of transporting data across the internet GRE provides the capability to transport routing protocols (for example: OSPF) that use broadcast and multicast.

18.2 Installing Licenses

There are three licenses that control access to the features:

- Basic VPN Management (`vpn_mgmt`)—allows users to manage a remote Black Box router.
- Firewall (`firewall`)—allows users to manage the firewall features. Also includes Basic VPN Management.
- Advanced VPN and firewall (`vpn_plus_firewall`)—Allows users to manage remote LANs. Also includes Basic VPN and Firewall licenses. Use this license to access the GRE features in this release.

To see the licenses available in this release, enter:

```
Blackbox/configure> system licenses ?

NAME
  licenses - Configure feature upgrade licenses

SYNTAX
  licenses license_type <cr>

DESCRIPTION
  license_type        -- Specifies the type of feature upgrade license
    The parameter may have any of the following values:
        enable_1_port -- Enable  1 port
        enable_2_ports-- Enable  2 ports
        enable_3_ports-- Enable  3 ports
        enable_4_ports-- Enable  4 ports
        BGP4          -- BGP4 routing
        vpn_mgmt      -- Enable VPN Mgmt License
        firewall      -- Enable Firewall and VPN Mgmt License
        vpn_plus_firewall-- Enable Advance VPN and Firewall License
```

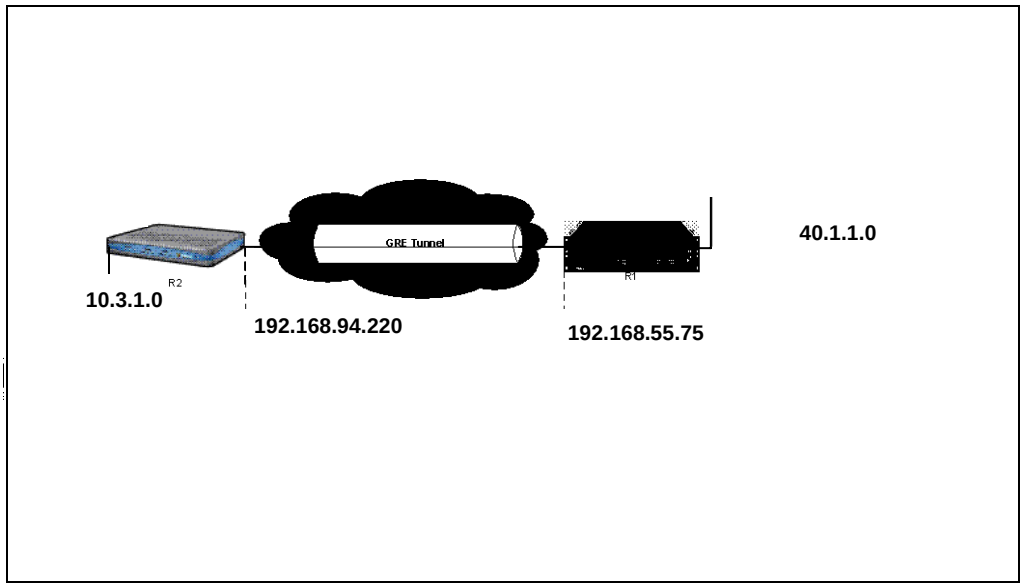
To install the advanced VPN and firewall license and use all the security features available in this release, enter:

```
Blackbox/configure> system licenses vpn_plus_firewall
Enter Security Upgrade License key: 024f3bc296b4ea7265
```

18.3 GRE Configuration Examples

This example explains how to configure a basic GRE tunnel as shown in Figure 36.

Figure 36 Fig 2 Simple GRE configuration



18.3.1Configuring Site to Site Tunnel

To configure GRE in a site to site tunnel configuration:

Step 1: Configure the interface.

```
Blackbox> configure terminal
Blackbox/configure> interface bundle wan1
Blackbox/configure/interface/bundle wan1> link t1 1
Blackbox/configure/interface/bundle wan1> encapsulation ppp
Blackbox/configure/interface/bundle wan1> ip address 192.168.94.220
255.255.255.0
Blackbox/configure/interface/bundle wan1> exit
```

Step 2: Configure the tunnel.

```
Blackbox/configure> interface tunnel t0
Blackbox/configure/interface/tunnel t0> ip 103.1.1.2 24
Blackbox/configure/interface/tunnel t0> tunnel source 192.168.94.220
Blackbox/configure/interface/tunnel t0> tunnel destination
192.168.55.75
Blackbox/configure/interface/tunnel t0> exit
```

Step 3: Configure the IP routes.

```
Blackbox/configure> ip route 0.0.0.0 0.0.0.0 192.168.94.254
Blackbox/configure> ip route 40.1.1.0 24 t0
```

NOTE

The peer of a local WAN interface cannot be used as a tunnel destination.

Step 4: Verify that the tunnel is up and running. (If it is not, check the **Gateway** and **Source Address** fields.)

```
Blackbox> show ip interface t0

t0 (unit number 5)
Type: TUNNEL
Flags: (0x74243) UP, RUNNING, MULTICAST-ROUTE
Internet Address: 103.1.1.2
Internet Netmask: 255.255.255.0
Internet Broadcast: 103.1.1.255
Maximum Transfer Unit: 1476 bytes
Source Address: 192.168.94.220
Destination Address: 192.168.55.75
Gateway: wan1
Protocol: GRE
Mac Address 00:50:52:60:00:00
```

For more information enter:

```
Blackbox> show interface tunnel t0

Tunnel: t0 Status: up
Internet Address: 103.1.1.2 Internet Netmask: 255.255.255.0
Source Address: 192.168.94.220 Destination Address: 192.168.55.75
MTU: 1476 bytes                    Protocol: GRE
ICMP unreachable: will be sent     ICMP redirect: will be sent
Crypto Snet: not set             Protection: policy grecisco key ****
TTL: 30                            Keepalive: disabled
TOS: not set                       Path MTU discovery: disabled
Key Value: not set                 Checksum: disabled
Sequence Datagrams: disabled

Tunnel Statistics:
    Bytes Rx                 95112    Bytes Tx                 60016
    Packets Rx                 860    Packets Tx                 499
    Err Packets Rx               0    Output Errs                  0
```

Step 5: Configure the Cisco side:

```
cisco > config t
cisco(config)#interface Ethernet2/0
cisco(config-if)#ip address 192.168.55.75255.255.255.0
cisco(config-if)#exit


cisco(config)#interface Tunnel 0
cisco(config-if)#ip address 103.1.1.1 255.255.255.0
cisco(config-if)#tunnel source 192.168.55.75
cisco(config-if)#tunnel destination 192.168.94.220
cisco(config-if)#exit

cisco(config)#ip route 0.0.0.0 0.0.0.0 192.168.55.254
cisco(config)#ip route 10.3.1.0 255.255.255.0 Tunnel0
```

18.4 Configuring GRE Site to Site with IPSec

This example extends the first example by adding encryption to the tunnel.

Step 1:Prepare the WAN link:

```
Blackbox> configure terminal
Blackbox/ configure> interface bundle wan1
Blackbox/ configure/interface/bundle wan1> link t1 1
Blackbox/ configure/interface/bundle wan1> encapsulation ppp
Blackbox/ configure/interface/bundle wan1> ip address 192.168.94.220 255.255.255.0
Blackbox/ configure/interface/bundle wan1> crypto untrusted
Blackbox/ configure/interface/bundle wan1> exit
```

Step 2: Configure the tunnel:

```
Blackbox/ configure> interface tunnel t0
Blackbox/ configure/interface/tunnel t0> ip address 103.1.1.2 24
Blackbox/ configure/interface/tunnel t0> tunnel source 192.168.94.220
Blackbox/ configure/interface/tunnel t0> tunnel destination 192.168.55.75
Blackbox/ configure/interface/tunnel t0> tunnel protection grecisco secretkeyfortest
Blackbox/ configure/interface/tunnel t0> crypto untrusted
Blackbox/ configure/interface/tunnel t0> exit
```

Step 3: Configure the routes:

```
Blackbox/ configure> ip route 0.0.0.0 0.0.0.0 192.168.94.254
Blackbox/ configure> ip route 40.1.1.0 24 t0
```

Step 4: Define the policy:

```
Blackbox/ configure > firewall internet
Blackbox/configure/firewall internet> policy 100 in proto gre self
Blackbox/configure/firewall internet/policy 100 in> exit
Blackbox/configure/firewall internet> policy 101 in service ike self
Blackbox/configure/firewall internet/policy 101 in> exit 2
Black Box configure> firewall corp
Blackbox/configure/firewall corp> policy 100 in self
```

Step 5: Check the status of the tunnel by entering:

```
Blackbox> show ip interface tunnel t0
```

Step 6:Validate the tunnel configuration by entering:

```
Blackbox> show crypto ipsec policy all
```

Or enter:

```
Blackbox> show crypto ike policy all
```

18.5 Configuring GRE Site to Site with IPSec and OSPF

This example extends the previous IPSec configuration example by enabling Open Shortest Path First (OSPF) protocol which provides redundant paths for the tunnel.

Step 1: To enable OSPF, add to the Black Box configuration above:

```
Blackbox> configure terminal
Blackbox/configure> router routerid 2.2.2.2
Blackbox/configure> router ospf
Blackbox/configure/router/ospf> interface t0 area 0
Blackbox/configure/router/ospf> exit
```

Step 2: Add to the Cisco configuration above

```
cisco > config t
cisco(config)#router ospf 1
cisco(config-router)# network 103.1.1.0 0.0.0.255 area 0
```

Step 3: To verify the OSPF configuration, enter:

```
Blackbox> show ip ospf interface all
```

NOTE

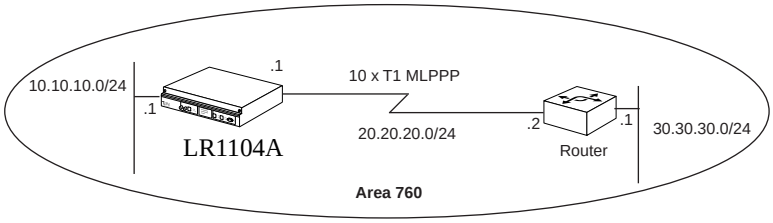
Using the redistribute connected command adds a recursive route to the tunnel destination. This will cause the tunnel to shut down. To prevent this, add a 32-bit static route for the tunnel destinatio**n.**

19
CONFIGURING OSPF AND FRAME RELAY

19.1 OSPF - Frame Relay

The following example shows OSPF running between a Black Box LR1112A and a router over a serial T1 link with back-to-back Frame Relay.

Figure 37 OSPF Over a Single T1 with Frame Relay



19.1.1Configuring the host name

```
LR1112A> configure terminal
LR1112A/configure> hostname LR1112A
```

19.1.2Configuring interface ethernet 0

```
LR1112A/configure> interface ethernet 0
LR1112A/configure/interface/ethernet0> ip address 10.10.10.1 24
LR1112A/configure/interface/ethernet0> exit
```

19.1.3Configuring interface bundle Dallas

```
LR1112A/configure> interface bundle Dallas
LR1112A/configure/interface/bundle Dallas> link t1 1
LR1112A/configure/interface/bundle Dallas> encapsulation frelay
LR1112A/configure/interface/bundle Dallas> fr
LR1112A/configure/interface/bundle Dallas/fr> intf_type dce
LR1112A/configure/interface/bundle Dallas/fr> pvc 16
LR1112A/configure/interface/bundle Dallas/fr/pvc 16> ip address 20.20.20.1
255.255.255.0
LR1112A/configure/interface/bundle Dallas/fr/pvc 16> exit 3
```

19.1.4Configuring OSPF

```
LR1112A/configure> router routerid 10.10.10.1
LR1112A/configure> router ospf
LR1112A/configure/router/ospf> area 760
LR1112A/configure/router/ospf/area 760> exit
```

19.1.5Configuring interface Dallas parameters

```
LR1112A/configure/router/ospf> interface Dallas dlci 16 area_id 760
LR1112A/configure/router/ospf/interface Dallas> cost 10
LR1112A/configure/router/ospf/interface Dallas> exit
```

19.1.6Configuring interface ethernet 0 parameters

```
LR1112A/configure/router/ospf> interface ethernet0 area_id 760
LR1112A/configure/router/ospf/interface ethernet0> cost 10
LR1112A/configure/router/ospf/interface ethernet0> exit 3
```

19.1.7Displaying OSPF parameters

Execute **show ip ospf int bundle** to display interface specific OPSPF parameters.

20
CONFIGURING PROTOCOL INDEPENDENT MULTICASTING ROUTING

20.1 PIM Configuration

Protocol Independent Multicast (PIM) protocols route multicast packets to multicast groups. PIM is protocol independent because it can leverage whichever unicast routing protocol is used to populate unicast routing table. There are two modes of PIM protocol – Dense mode (DM) and Sparse mode (SM). Black Box supports SM only.

PIM-DM floods multicast traffic throughout the network initially and then generates prune messages as required. PIM-SM attempts to send multicast data only to networks which have active receivers. This is achieved by having a common Rendezvous Point (RP) known to the senders and receivers and by forming shared trees from the RP to the receivers.

PIM-SM is described in RFC 2362.

20.1.1PIM Commands

The general PIM commands supported in this release are:

Global parameters

Enable PIM	Blackbox/configure/ip> pim
Configure PIM mode	Blackbox/configure/ip/pim> mode [sparse | dense]
Configure Assert Holdtime	Blackbox/configure/ip/pim>assert-holdtime <time>
Configure Hello Interval	Blackbox/configure/ip/pim>hello-interval <time>
Configure Hello Holdtime	Blackbox/configure/ip/pim>hello-holdtime <time>
Configure Hello priority	Blackbox/configure/ip/pim>hello-priority <value>
Configure Join/Prune Holdtime	Blackbox/configure/ip/pim>join-prune-holdtime <time>
Configure Join /Prune Interval	Blackbox/configure/ip/pim>join-prune-interval <time>
Configure MRT Period	Blackbox/configure/ip/pim>mrt-period <time>

Configure MRT Stale Multiplier	Blackbox/configure/ip/pim>mrt-stale-mult <number>
Configure MRT SPT Multiplier	Blackbox/configure/ip/pim>mrt-spt-multiplier <number>
Configure Probe Period	Blackbox/configure/ip/pim>probe-period <time>
Configure Registration suppression timeout	Blackbox/configure/ip/pim>register-suppress-timeout <time>
Configure DR to switch immediate	Blackbox/configure/ip/pim>dr-switch-immediate
Configure RP to switch immediate	Blackbox/configure/ip/pim>rp-switch-immediate
Configure Threshold for DR	Blackbox/configure/ip/pim>threshold-dr <bps>
Configure Threshold for RP	Blackbox/configure/ip/pim>threshold-rp <bps>
Configure to calculate whole packet checksum (for cisco interop)	Blackbox/configure/ip/pim>whole-packet-checksum
Bootstrap Router related Commands	
Configure as candidate BSR	Blackbox/configure/ip/pim/cbsr> address <address>
Configure CBSR period	Blackbox/configure/ip/pim/cbsr> period <time>
Configure CBSR holdtime	Blackbox/configure/ip/pim/cbsr>holdtime <time>
Configure CBSR priority	Blackbox/configure/ip/pim/cbsr>priority <value>
RP commands	
Configure as candidate RP	Blackbox/configure/ip/pim>crp
Configure as candidate RP address	Blackbox/configure/ip/pim/crp> address <ipaddress>
Configure candidate RP group for advertisement	Blackbox/configure/ip/pim/crp> group-add <address> [mask] [priority]
Configure as candidate RP holdtime	Blackbox/configure/ip/pim/crp>holdtime <time>
Configure as candidate RP period	Blackbox/configure/ip/pim/crp>period <time>
Configure as candidate RP priority	Blackbox/configure/ip/pim/crp>priority <value>
Configure a static RP address	Blackbox/configure/ip/pim/> rp <address> <gaddress> [mask]
Inteface based parameters	
Configure PIM for an interface	Blackbox/configure/ip/pim>interface <interface_name>[:dlci_no]
Configure PIM mode for an interface	Blackbox/configure/ip/pim/interface wan1> mode [sparse | dense | ssm | sparse-ssm]

Configure PIM interface assert holdtime	Blackbox/configure/ip/pim/interface wan1>assert-holdtime <time>
Configure PIM interface hello holdtime	Blackbox/configure/ip/pim/interface wan1>hello-holdtime <time>
Configure PIM interface hello interval	Blackbox/configure/ip/pim/interface wan1>hello-interval <time>
Configure PIM interface Join/Prune Delay Timeout	Blackbox/configure/ip/pim/interface wan1>join-prune-timeout <time>
Configure PIM interface Join/Prune Interval	Blackbox/configure/ip/pim/interface wan1>join-prune-interval <time>
Configure PIM interface Join/Prune holdtime	Blackbox/configure/ip/pim/interface wan1>join-prune-holdtime <time>
Configure PIM interface as border of PIM domain	Blackbox/configure/ip/pim/interface wan1>boundary

PIM SSM

Configure the SSM range	Blackbox/configure/ip/pim> ssm-range <group-address> <group-mask

The show and debug PIM commands are:

Display PIM global configuration	Blackbox>show ip pim global
Display PIMC timers	Blackbox>show ip pim timers
Display PIM interfaces	Blackbox>show ip pim interfaces
Display PIM neighbors	Blackbox>show ip pim neighbors
Display PIM Bootstrap info	Blackbox>show ip pim bsr-info
Display PIM Candidate RP info	Blackbox>show ip pim crp-info
Display PIM statistics	Blackbox>show ip pim statistics
Display PIM RP set	Blackbox>show ip pim rp-set
Display PIM Static RP	Blackbox>show ip pim rp

Trace PIM packets	Blackbox> debug ip pim packet <pkt_type> <direction> [interface_name] [dlci]
Trace PIM state changes	Blackbox> debug ip pim state
Trace PIM routes	Blackbox> debug ip pim route
Trace PIM detail	Blackbox> debug ip pim detail
Trace PIM debug	Blackbox> debug ip pim debug
All Traces	Blackbox>debug ip pim all

20.1.2PIM Configuration Examples

This section shows examples of how the PIM commands are used.

To access PIM mode, enter:

```
Blackbox/configure/ip> pim
Blackbox/configure/ip/pim>
```

The following example enters the BSR mode.

```
Blackbox/configure/ip/pim> cbsr
Blackbox/configure/ip/pim/cbsr>
```

The following command sets Ethernet1 as the BSR interface.

```
Blackbox/configure/ip/pim/cbsr> interface ethernet1
```

The following example sets the holdtime to 33 seconds.

```
Blackbox/configure/ip/pim/cbsr> holdtime 33
Blackbox/configure/ip/pim/cbsr>
```

To configure the DLCI for Ethernet0 to 100, enter:

```
Blackbox/configure/ip/pim/cbsr> interface ethernet0 dlci 100
```

To set the CBSR priority to 45, enter:

```
Blackbox/configure/ip/pim/cbsr> priority 45
```

To enter the candidate Rendezvous Point mode, enter:

```
Blackbox/configure/ip/pim> crp
Blackbox/configure/ip/pim/crp>
```

To set the group IP address for CRP advertisements to 224.1.1.0, enter:

```
Blackbox/configure/ip/pim/crp> group-add 224.1.1.0
```

To set the flag at the DR to switch to the SPT on receiving the first packet (default on), enter:

```
Blackbox/configure/ip/pim> dr-switch-immediate
```

The following example configures the MRT SPT Mult value to be 25.

```
Blackbox/configure/ip/pim> mrt-spt-mult 25
```

The following example configures the probe period to 30 seconds.

```
Blackbox/configure/ip/pim> probe-period 30
Blackbox/configure/ip/pim>
```

The following example configures the Register Suppression Timeout to be 70 seconds.

```
Blackbox/configure/ip/pim> register-suppress-timeout 70
```

To set the RP static IP address to 10.10.1.1, enter:

```
Blackbox/configure/ip/pim> rp 10.10.1.1
```

To set the flag for the RP to switch to the SPT for (S,G) upon receipt of the first Register message (default: on). To turn on this feature, enter:

```
Blackbox/configure/ip/pim> rp-switch-immediate
```

The following example configures this feature.

```
Blackbox/configure/ip/pim> rp-switch-immediate
```

To configure the router such that the data from S addressed to G must exceed an average of 1024 KBytes per second before an SPT switch is initiated, enter:

```
Blackbox/configure/ip/pim> threshold-dr 1024
```

To configure the threshold-dr option such that the data from S addressed to G must exceed an average of 1500 KBytes per second before an SPT switch is initiated. If this router is a DR for the pair (S,G), then the same data must exceed an average of 1500 KBytes per second before an SPT switch is initiated. The period over which the average will be calculated will be the **mrt-period** times the **mrt-spt-mult**, or 60 seconds.

```
Blackbox/configure/ip/pim> threshold-rp 1500
```

To specify that the message checksum will be calculated over the entire encapsulated packet, rather than just over the Register message header, enter:

```
Blackbox/configure/ip/pim> whole-packet-checksum
```

The following example configures a global assert-holdtime value of 600.

```
Blackbox/configure/ip/pim> assert-holdtime 600
```

To set the holdtime to 60 seconds, enter:

```
Blackbox/configure/ip/pim> hello-holdtime 60
```

To set the hello interval time to 145 seconds, enter:

```
Blackbox/configure/ip/pim> hello-interval 145
```

To set the priority to 15, enter:

```
Blackbox/configure/ip/pim> hello-priority 15
```

To set the holdtime to 30 seconds, enter:

```
Blackbox/configure/ip/pim> join-prune-holdtime 30
```

To send messages every five minutes, enter:

```
Blackbox/configure/ip/pim> join-prune-interval 300
```

To check the router table every 15 seconds, enter:

```
Blackbox/configure/ip/pim> mrt-period 15
```

To set the `mrt-spt-mult` value to be ten times that of the `mrt-period` value, enter:

```
Blackbox/configure/ip/pim> mrt-spt-mult 10
```

To set the time out (S, G) entries at 5 times the mrt-period value, enter:

```
Blackbox/configure/ip/pim> mrt-stale-mult 5
```

To display PIM global configuration settings, enter:

```
Blackbox/configure> display ip pim global
PIM: Enabled
        Mode: Sparse
        Timers:
                Hello Interval: 145
                Hello Hold Time: 60
                Hello Priority: 15

                Join/Prune Interval: 300
                Join/Prune Hold Time: 30
                Assert Hold Time: 200
                Probe Period: 15
                Register Suppress Timeout: 90
                MRT Interval: 15
                MRT SPT Multiplier : 10
                MRT Stale Multiplier: 5
        Thresholds:
                Threshold DR: 2400
                Threshold RP: 1500
        RP Switch Immediate: enabled
        DR Switch Immediate: enabled
        Whole packet checksum: enabled
        SSM Range: 224.20.12.1 24
Blackbox/configure>
```

To display information for all interfaces, enter:

```
Blackbox/configure> display ip pim interface all
```

To see all IP PIM interface information for Ethernet1, enter:

```
Blackbox/configure/ip/pim/interface ethernet1> display ip pim interface ethernet1
```

To display IP PIM statistics for ethernet1, enter:

```
Blackbox/configure/ip/pim/interface ethernet1> display ip pim statistics
PIM Statistics:
                     Total PIM msgs recvd  0 (0 bytes)
                     Recvd msgs too short  0
                  Recvd msgs bad checksum  0
                  Recvd msgsg bad version  0
                      Recvd register msgs  0 (0 bytes)
                Recvd registers wrong iif  0
                      Recvd bad registers  0
                       Sent register msgs  0 (0 bytes)


Blackbox/configure/ip/pim/interface ethernet1>
```

To display information on PIM neighbors, enter:

```
Blackbox/configure> display ip pim neighbors
Neighbor       Interface     Uptime   Expires         Hello Priority
-------------- ------------ -------- --------------- --------------
Blackbox/configure>
```

To display RP information, enter:

```
Blackbox/configure> display ip pim rp
        Group/Mask         RP
        ------------------ ---------------
        224.0.0.0/4        10.10.1.1
Blackbox/configure>
```

To view RP-set information, enter:

```
Blackbox/configure> display ip pim rp-set
Group/mask         Src/RP           Pri Uptime     Expires
----------         ------           --- ------     -------
224/4              10.10.1.1        1   Static RP
  Dependencies:    None

Blackbox/configure>
```

To view PIM counters, enter:

```
Blackbox/configure> display ip pim statistics
PIM Statistics:
                     Total PIM msgs recvd  0 (0 bytes)
                     Recvd msgs too short  0
                  Recvd msgs bad checksum  0
                  Recvd msgsg bad version  0
                      Recvd register msgs  0 (0 bytes)
                Recvd registers wrong iif  0
                      Recvd bad registers  0
                       Sent register msgs  0 (0 bytes)
Blackbox/configure>
```

To display PIM timer information, enter:

```
Blackbox/configure> display ip pim timers
PIM Timers:
        Hello Interval: 145
        Hello Hold Time: 60
        Hello Priority: 15

        Join/Prune Interval: 300
        Join/Prune Hold Time: 30
        Assert Hold Time: 200
        Probe Period: 15
        Register Suppress Timeout: 90
        MRT Interval: 15
        MRT SPT Multiplier : 10
        MRT Stale Multiplier: 5
Blackbox/configure>
```

To examine PIM BSR statistics, enter:

```
Blackbox/configure/ip/pim> display ip pim bsr-info
Candidate BSR Information
-------------------------
Candidate BSR Status: Disabled
Candidate BSR Interface: NOT CONFIGURED
        Candidate BSR Priority: 45
        Candidate BSR Period: 30

        Candidate BSR Hold Time: 2048
        Candidate BSR Admin Scope: Disabled

No BSR's
Blackbox/configure/ip/pim>
```

To reset PIM counters, enter:

```
Blackbox> clear ip pim statistics
```

21
MTRACE CONFIGURATION

21.1 Multicast Traceroute Facility

With multicast distribution trees, tracing from a source to a multicast destination is difficult, since the branch of the multicast tree on which the destination lies is unknown. The technique used by the **traceroute** tool to trace unicast network paths will not work for IP multicast because traceroute (ICMP) responses are specifically forbidden for multicast traffic. Thus, you have to flood the whole tree to find the path from one source to one destination. However, walking up the tree from destination to source is easy, as most existing multicast routing protocols know the previous hop for each source. Tracing from destination to source involves only routers on the direct path.

To request a traceroute (which does not have to be the source or the destination), send a traceroute query packet to the last-hop multicast router for the given destination. The last-hop router turns the query into a request packet by adding a response data block containing its interface addresses and packet statistics, and then forwards the request packet using unicast to the router that it believes is the proper previous hop for the given source and group. Each hop adds its response data to the end of the request packet, then unicast forwards it to the previous hop. The first hop router (the router that believes that packets from the source originate on one of its directly connected networks) changes the packet type to indicate a response packet and sends the completed response to the response destination address. The response may be returned before reaching the first hop router if a fatal error condition such as “no route” is encountered along the path.

Multicast traceroute uses any information available to it in the router to try to determine a previous hop to forward the trace towards. Multicast routing protocols vary in the type and amount of state they keep; multicast traceroute tries to work with all of them by using whatever is available. For example, if a DVMRP router has no active state for a particular source but does have a DVMRP route, it chooses the parent of the DVMRP route as the previous hop. If a PIM-SM router is on the (*,G) tree, it chooses the parent towards the RP as the previous hop. In these cases, no source/group-specific state is available, but the path may still be traced.

Black Box supports the following PIM related feature—a “traceroute” facility for IP multicast, as defined in draft-ietf-idmr-traceroute-ipm-05.

The **mtrace** command for multicast traffic is similar to the **traceroute** command used for unicast traffic. Unlike **traceroute**, however, **mtrace** traces traffic backwards, from the receiver to the source. **mtrace** uses other unicast routing tables for RPF. For these, **mtrace** relies on Black Box Networks’ implementation of the **mtrace** protocol is manageable through the CLI and can be executed from any command sub-tree of the Black Box CLI.

21.1.1 mtrace Command

mtrace

21.1.2 Restrictions

In this release, configuring Maximum Hops & TTL is not permitted.

Maximum hops is set to 32 and TTL is set to 127 in all **mtrace** packets as default.

For **mtrace** to work:

- IGMP must be enabled in the router
- IGMP should be enabled on at least one interface.

21.1.2 mtrace Example

Traceroute using **mtrace** from 192.168.0.0 to 192.168.2.22 through group 225.254.254.254

```
Blackbox> mtrace 192.168.0.0 192.168.2.22 239.254.254.254

mtrace from 192.168.2.0 to 192.168.2.22 through group 225.254.254.254
Querying full reverse path...
 1  192.168.2.15 PIM  thresh^ 0  0 ms
 2  192.168.2.7 PIM  thresh^ 0  2 ms
 3  192.168.2.5 PIM  thresh^ 0  674 ms
 4  192.168.2.3 PIM  thresh^ 0  673 ms
 5  192.168.2.2 PIM  thresh^ 0  674 ms
 6  192.168.2.1 PIM  thresh^ 0  673 ms
```

Where in the line `4  192.168.2.3 PIM  thresh^ 0  673 ms`:

192.168.2.3 is the intermediate router 4 hops away from the destination.

Multicast Protocol in use on this hop and TTL Threshold.

673 ms is the time taken to trace to be forwarded between hops.

22
CONFIGURING QUALITY OF SERVICE ROUTING

22.1 Configuring QoS

Black Box QoS ensures bandwidth guarantees throughout the system by implementing Random Early Detection (RED) to address congestion and Class Based Queuing (CBQ) to address traffic policing. This document discusses the CBQ features.

Black Box's bandwidth management capability allows multiple agencies or customers to share access bandwidth on a WAN link in a controlled fashion to effectively and efficiently utilize available bandwidth. Even during times of congestion, each customer is guaranteed a share of the access bandwidth and is allowed to borrow unused bandwidth from other customers. This bandwidth management capability allows service providers to offer their customers Internet access based on the amount of guaranteed bandwidth-committed rate (CR) and the amount of bandwidth-borrowed burst rate (BR). Similarly, an organization can share its access bandwidth among its different departments.

22.1.1Features

The network administrator manages bundle bandwidth across various customers by defining traffic classes. Each traffic class is assigned the desired committed bandwidth as well as the burst bandwidth. The sum of the CRs of all classes must be less than or equal to the total bundle bandwidth. CBQ can be deployed in both the WAN outbound and WAN inbound directions.

A traffic class is characterized by the following parameters:

- Class name
- Parent class
- Committed rate (CR)
- Burst rate (BR)
- Classification type based on:
  - Application level
    - Application ports (TCP or UDP)
  - Network level
    - Source or destination IP addresses, address ranges, or subnets
  - Ethernet MAC level
    - VLAN identifiers

Traffic classes are arranged in a hierarchical manner. A class has a parent class and can have one or more child classes. The root class has no parent and is identified as *root-out* or *root-in*. There is no theoretical limit to the number of classes that can be created. The only limitation that can arise is due to available memory in the Black Box system.

22.1.2Definitions

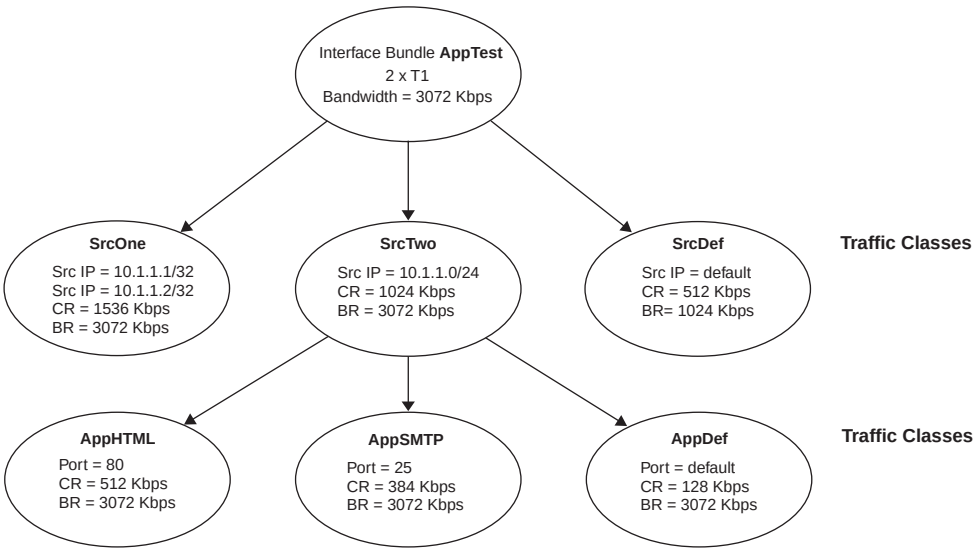
- Committed Rate
  Each traffic class can be assigned a CR parameter in Kbps. This is the amount of bandwidth that the class or flow is guaranteed at all times, even during congestion. The sum of the CRs for all classes in a given direction cannot exceed the access bandwidth of their parent class. By maintaining a moving average of the bandwidth for each class, the class is not “strictly” policed at CR Kbps, and momentary bursts in the flow are permitted. The goal is that each class with sufficient demand will be able to receive roughly its allocated bandwidth over some interval of time.
- Burst Rate
  Every traffic class can be configured with a burst parameter, which is the bandwidth that can be offered to that class if unused bandwidth is available from other classes. This provides for very efficient bandwidth utilization. A class can also be configured to borrow whatever bandwidth is available from its parent class up to the BR limit set for that class. To prevent a class from borrowing, set the CR equal to the BR. Also, note that a class cannot borrow more than the bundle bandwidth.

22.1.3Classification Types

The example in Figure 1 reserves the largest CR (1536 Kbps) for two servers, 10.1.1.1 and 10.1.1.2, which are members of the SrcOne class. The remainder of the 10.1.1.0/24 subnet is assigned to the SrcTwo class and is configured with a CR of 1024 Kbps. Additionally, the SrcTwo class is further divided into application port classes. All other hosts in Figure 1, the default class, are configured for a CR of 512 Kbps.

The classification type must be the same across a given level of traffic class. Note in Figure 1, that the classification type at the first level traffic class is the source IP address; for the second level, the classification type is the application port. Because bandwidth limitations are evaluated from most specific to least specific, 10.1.1.1/32 falls within the SrcOne class.

Figure 38 Assigning Classification Types



Configuration for the example in Figure 38:

22.1.3.1 Create bundle AppTest

```
LR1104A/configure> interface bundle AppTest
LR1104A/configure/interface/bundle AppTest> link ct3 1 18-19
LR1104A/configure/interface/bundle AppTest> encap ppp
LR1104A/configure/interface/bundle AppTest> ip addr 199.1.1.1 255.255.255.252
```

22.1.3.2 Create traffic classes

```
LR1104A/configure/interface/bundle AppTest> qos
LR1104A/configure/interface/bundle AppTest/qos> add_class SrcOne root-out cr 1536 br 3072
LR1104A/configure/interface/bundle AppTest/qos> add_class SrcTwo root-out cr 1024 br 3072
LR1104A/configure/interface/bundle AppTest/qos> add_class SrcDef root-out cr 512 br 1024
LR1104A/configure/interface/bundle AppTest/qos> add_class AppHTML SrcTwo cr 512 br 3072
LR1104A/configure/interface/bundle AppTest/qos> add_class AppSMTP SrcTwo cr 384 br 3072
LR1104A/configure/interface/bundle AppTest/qos> add_class AppDef SrcTwo cr 128 br 3072
```

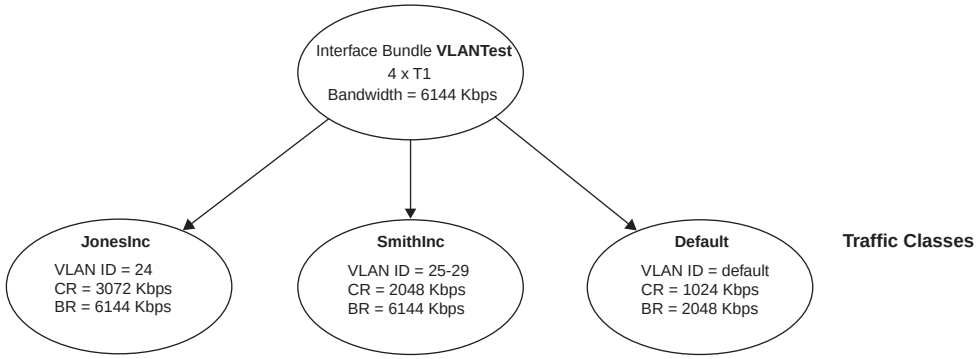
22.1.3.3 Assign classification types

```
LR1104A/configure/interface/bundle AppTest/qos> class SrcOne
LR1104A/configure/interface/bundle AppTest/qos/class SrcOne> add_src_ip 10.1.1.1
255.255.255.255
LR1104A/configure/interface/bundle AppTest/qos/class SrcOne> add_src_ip 10.1.1.2
255.255.255.255
LR1104A/configure/interface/bundle AppTest/qos/class SrcOne> exit
LR1104A/configure/interface/bundle AppTest/qos> class SrcTwo
LR1104A/configure/interface/bundle AppTest/qos/class SrcTwo> add_src_ip 10.1.1.0
255.255.255.0
LR1104A/configure/interface/bundle AppTest/qos/class SrcTwo> exit
LR1104A/configure/interface/bundle AppTest/qos> class SrcDef
LR1104A/configure/interface/bundle AppTest/qos/class SrcDef> add_src_ip default
LR1104A/configure/interface/bundle AppTest/qos/class SrcDef> exit
LR1104A/configure/interface/bundle AppTest/qos> class AppHTML
LR1104A/configure/interface/bundle AppTest/qos/class AppHTML> add_port 80
LR1104A/configure/interface/bundle AppTest/qos/class AppHTML> exit
LR1104A/configure/interface/bundle AppTest/qos> class AppSMTP
LR1104A/configure/interface/bundle AppTest/qos/class AppSMTP> add_port 25
LR1104A/configure/interface/bundle AppTest/qos/class AppSMTP> exit
LR1104A/configure/interface/bundle AppTest/qos> class AppDef
LR1104A/configure/interface/bundle AppTest/qos/class AppDef> add_port default
LR1104A/configure/interface/bundle AppTest/qos/class AppDef> exit
LR1104A/configure/interface/bundle AppTest/qos> enable
LR1104A/configure/interface/bundle AppTest/qos> exit 3
```

22.1.4 VLAN Identifiers

Figure 2 illustrates the classification based on VLAN identifiers. Note that these classes are leaf classes and do not have child classes.

Figure 39 Assigning VLAN Identifiers



Configuration for Figure 39:

22.1.4.1 Create bundle VLANtest

```
LR1104A> conf t
LR1104A/configure> interface bundle VLANtest
LR1104A/configure/interface/bundle VLANtest> link ct3 1 20-23
LR1104A/configure/interface/bundle VLANtest> encap ppp
LR1104A/configure/interface/bundle VLANtest> ip addr 200.1.1.1 255.255.255.252
```

22.1.4.2 Create traffic classes and assign classifications

```
LR1104A/configure/interface/bundle VLANtest> qos
LR1104A/configure/interface/bundle VLANtest/qos> add_class JonesInc root-out cr 3072 br 6144
LR1104A/configure/interface/bundle VLANtest/qos> add_class SmithInc root-out cr 2048 br 6144
LR1104A/configure/interface/bundle VLANtest/qos> add_class Default root-out cr 1024 br 2048
LR1104A/configure/interface/bundle VLANtest/qos> class JonesInc
LR1104A/configure/interface/bundle VLANtest/qos/class JonesInc> add_vlan_id 24
LR1104A/configure/interface/bundle VLANtest/qos/class JonesInc> exit
LR1104A/configure/interface/bundle VLANtest/qos> class SmithInc
LR1104A/configure/interface/bundle VLANtest/qos/class SmithInc> add_vlan_id 25-29
LR1104A/configure/interface/bundle VLANtest/qos/class SmithInc> exit
LR1104A/configure/interface/bundle VLANtest/qos> class Default
LR1104A/configure/interface/bundle VLANtest/qos/class Default> add_vlan_id default
LR1104A/configure/interface/bundle VLANtest/qos/class Default> exit
LR1104A/configure/interface/bundle VLANtest/qos> enable
LR1104A/configure/interface/bundle VLANtest/qos> exit 4
```

22.1.5Bulk Statistics

The Bulk statistics command enables users to collect statistics for every N hours (N <4 hours) and upload the statistics for every class to an FTP server. The data is sent in an ASCII format file with three sections. The first section includes the upload time, system IP address, sample interval in minutes, and the upload interval in minutes. The second section includes class-based statistics for all bundles configured and enabled with QoS. The third section includes class-based statistics. Empty lines and header lines in the file start with the "#" character. The bundle statistics start with the character "B," and class statistics start with the character "C." These designations allow easier parsing of the file.

22.1.5.1 Configuring bulk statistics

```
LR1104A/configure/.../qos> bulk_stats_ftp
Primary FTP server: 10.1.3.1
Secondary FTP server: 10.1.18.1
FTP user name: bjones
FTP password: xxxxxxxx
LR1104A/configure/.../qos> bulk_statistics sample_interval 5 upload_interval 1
LR1104A/configure/.../qos> show qos bulkstats_config
```

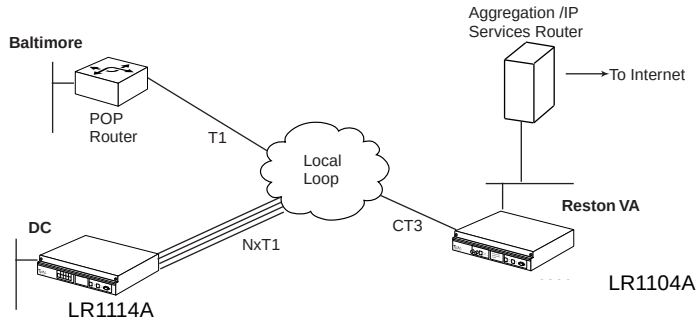
Figure 40 Screen Display for show qos bulkstats_config Command

```
Bulk Statistics Configuration
-----------------------------

status                : ENABLED
Primary FTP server    : 10.10.1.1
Secondary FTP server  : 10.2.2.1
FTP user name         : joeuser
FTP password          : ******
Upload interval       : 1 hrs
Sample interval       : 5 mins
```

23
VIRTUAL LAN TAGGING

23.1 Managing Traffic with VLAN Tagging

Figure 41 Aggregation Using VLAN Tagging



The illustration above shows two customers connected to an aggregation/IP services router using a Black Box LR1104A. All packets coming into the Black Box LR1104A on the single T1 bundle are tagged with VLAN ID 5. All packets coming across the 4 T1 bundle from DC are tagged with a VLAN tag of 10.

In this example, the VLAN tags are only relevant from the Black Box LR1104A to the VLAN-enabled POP router. The tags are removed in the reverse direction. Black Box's IP multiplexing technology enables both remote customers to operate as if they are directly connected to the POP router residing on a tagged VLAN. In this scenario, the provider can offer HDLC, PPP, MLPPP, frame relay, and MFR connections. (The sample configurations in this document assume Baltimore uses frame relay and DC uses MLPPP.) Upgrading customer service by adding T1s to a Black Box product can be accomplished remotely (for example, at DC) after the T1 cable has been connected. Thus, deploying a technician to reconfigure the unit is not necessary.

By connecting the Black Box LR1104A using a VLAN switch, additional LR1104As and POP routers can be easily added. If additional LR1104As are desired, the appropriate uplink from the VLAN switch is Gigabit Ethernet. Redundancy for the POP routers can be provided using either the second fast Ethernet port on the LR1104A, in conjunction with Black Box's failover feature, or using HSRP/VRRP between the two routers. In the latter case, a VLAN switch is required.

Special configuration is not required at the CPE for this application. At the POP, traffic from each bundle or frame relay PVC is tagged and forwarded to a VLAN trunk port on the Ethernet interface. In the other direction, the Black Box LR1104A proxies for the CPE routers after learning their IP addresses via link control protocol or inverse ARP. Routing between customer VLANs, firewall functions, and traffic management can be provided by the POP router sub-interfaces so there is only one location to monitor customer traffic.

In this example application, the POP router is configured with the following three sub-interfaces:

- 205.1.1.1
- 205.1.1.5
- 10.1.1.5

23.1.1 Reston configuration: Black Box LR1104A

```
LR1104A/configure> hostname reston
reston/configure> no ftp_server
reston/configure> no autoconf
```

23.1.1.1 Configure interface bundle balt1

```
reston/configure> interface bundle balt1
reston/configure/interface/balt1> link ct3 1 1
reston/configure/interface/balt1> encapsulation fr
reston/configure/interface/balt1> fr
reston/configure/interface/balt1/fr> intf_type dce
```

23.1.1.2 Configure interface balt1 pvc 100

```
reston/configure/interface/balt1/fr> pvc 100
reston/configure/interface/balt1/fr/pvc 100> policing cir 1536000 bc 1536000 be
1536000
reston/configure/interface/balt1/fr/pvc 100> shaping cir 1536000 bcmax 1536000 bcmin
1536000 be 1536000
```

 # The Baltimore router is 205.1.1.2/30.

 # The PVC uses a private address on the Reston end.

```
reston/configure/interface/balt1/fr/pvc 100> ip addr 10.1.1.1 255.255.255.252
```

 # The POP router is 205.1.1.1/30

```
reston/configure/interface/balt1/fr/pvc 100> ip source_forwarding 205.1.1.1
reston/configure/interface/balt1/fr/pvc 100> vlan
reston/configure/interface/balt1/fr/pvc 100/vlan> vlanid 5
reston/configure/interface/balt1/fr/pvc 100/vlan> exit 4
```

23.1.1.3 Configure interface bundle dc1

```
reston/configure> interface bundle dc1
reston/configure/interface/bundle dc1> link ct3 1 2-5
reston/configure/interface/bundle dc1> encapsulation ppp
reston/configure/interface/bundle dc1> ip unnumbered ethernet0
```

 # DC is 205.1.1.6/30.

```
reston/configure/interface/bundle dc1> ip source_forwarding 205.1.1.5
reston/configure/interface/bundle dc1> vlan
reston/configure/interface/bundle dc1>/vlan> vlanid 10
reston/configure/interface/bundle dc1>/vlan> exit 2
```

23.1.1.4 Configure interface ethernet 0

```
reston/configure> interface ethernet 0
reston/configure/interface/ethernet0> speed 100 full_duplex
reston/configure/interface/ethernet0> ip address 10.1.1.6 255.255.255.252
reston/configure/interface/ethernet0> exit
```

23.1.1.5 Configure ip routing

```
reston/configure> ip
reston/configure/ip> route 205.1.1.0 255.255.255.0 ethernet0 1
reston/configure/ip> route 0.0.0.0 0.0.0.0 10.1.1.5 1
reston/configure/ip> exit
```

 # The above route summarizes the customer access subnets.

23.1.2 DC configuration: Black Box LR1114A

```
Blackbox> configure terminal
Blackbox/configure> hostname dc1
dc1/configure>
```

23.1.2.1 Configure interface ethernet 0

```
dc1/configure> interface ethernet 0
dc1/configure/interface/ethernet0> ip addr 205.100.1.1 255.255.255.0
dc1/configure/interface/ethernet0> exit
```

23.1.2.2 Configure interface bundle mip

```
dc1/configure> interface bundle mlp
dc1/configure/interface/bundle mlp> link t1 1-4
dc1/configure/interface/bundle mlp> encapsulation ppp
dc1/configure/interface/bundle mlp> ip addr 205.1.1.6 255.255.255.252
dc1/configure/interface/bundle mlp> exit
```

23.1.2.3 Configure ip routing

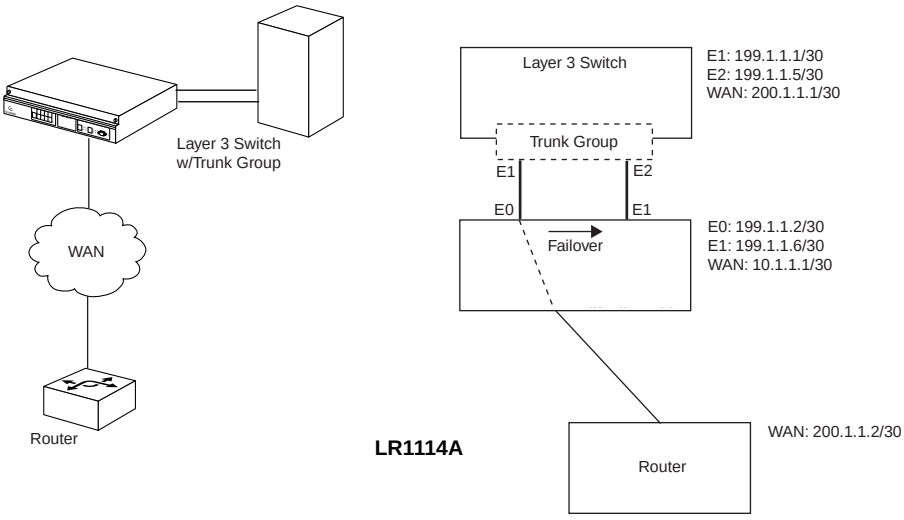
```
dc1/configure> ip
dc1/configure/ip> routing
dc1/configure/ip> route 0.0.0.0 0.0.0.0 205.1.1.5 1
dc1/configure/ip> exit
dc1/configure>
```

24
MANAGING REDUNDANT CONNECTIONS

24.1 Trunk Group/Failover

Redundant connections are often required between Black Box systems and the switches to which they connect. The following diagram illustrates Ethernet redundancy between a Black Box LR1114A and a Layer 3 switch using failover on the Black Box and a trunk group configuration on the switch.

Figure 42 Trunk Group/Failover Configuration



24.1.1 Configuration Details

- Black Box Ethernet 0 and 1 are connected to ports 1 and 2 of a trunk group configured switch.
- The trunk group is configured with three IP addresses and a single MAC address. One IP address is utilized for WAN connectivity; the second address provides for communication between the switch and Black Box Ethernet 0. For this configuration, a third IP address is utilized for the failover path.
- The Black Box LR1114A is configured for failover on E0. When E0 loses link conectivity, it will failover to E1 and continue to pass traffic. When E0 recovers, traffic will be switched back.

- The Black Box LR1114A is connected to a router via a bundle “WAN” (T1 PPP bundle) in IPMux mode.
- To manage the Black Box LR1114A from the switch during normal mode, ping, telnet, or snmp to the Ethernet 0 IP address; during failover mode, ping, telnet, or snmp to the Ethernet 1 IP address.

24.1.1.1 Configure the Black Box LR1114A for Failover Operation

```
Blackbox> configure term
Blackbox/configure> interface ethernet 0
Blackbox/configure/interface/ethernet> ip address 199.1.1.2 255.255.255.252
Blackbox/configure/interface/ethernet> failover
Blackbox/configure/interface/ethernet> exit

Blackbox/configure> interface ethernet 1
Blackbox/configure/interface/ethernet> ip address 199.1.1.1.6 255.255.255.252
Blackbox/configure/interface/ethernet> exit

Blackbox/configure> interface bundle wan
Blackbox/configure/interface/bundle> link t1 1
Blackbox/configure/interface/bundle> enc ppp
Blackbox/configure/interface/bundle> ip address 10.1.1.1 255.255.255.252
Blackbox/configure/interface/bundle> ipmux source_forwarding 199.1.1.1
Blackbox/configure/interface/bundle> exit
```

25
WAN INTERFACE CONFIGURATIONS

25.1 T1 Interface Configuration

Black Box systems are available with T1 WAN interfaces. Consult the Black Box *System Installation Guide* for details on WAN interface types, cabling, and pinouts.

This document outlines the configuration of module parameters (Layer 1) and, to a lesser degree, the configuration of bundle parameters (Layer 2). The bundle configuration examples demonstrate linking of physical interfaces (modules) to logical interfaces (bundles). Module configuration occurs within the **configure module** tree of the Black Box CLI, and bundle configuration occurs within the **configure interface bundle** tree.

Black Box T1 interfaces support logical interfaces made up of fractional T1, single T1, and multi-link T1connections.

25.1.1Module Configuration

25.1.1.1 T1

The following example configures the operational and descriptive parameters for T1 number 6.

Configure T1 Parameters

```
Blackbox/configure> module t1 6
Blackbox/configure/module/t1> circuitId X1234567890
Blackbox/configure/module/t1> contactInfo George_Anderson
Blackbox/configure/module/t1> description T1_to_Troy
Blackbox/configure/module/t1> framing esf
Blackbox/configure/module/t1> linecode b8zs
Blackbox/configure/module/t1> clock_source line
Blackbox/configure/module/t1> exit
```

25.1.2 Bundle Configuration

Configuration of an interface bundle is required for use of any of the Black Box system WAN interfaces. Multiple physical interfaces may be linked to a single interface bundle; multi-link protocols, including MLPPP and Multilink Frame Relay, make use of NxT1 interfaces to create single logical interfaces.

The interface bundle specifies the physical connection(s) to be linked, an encapsulation protocol (Layer 2) and, optionally, Layer 3 parameters.

25.1.2.1 Fractional T1

The following example creates a 384 Kbps fractional T1 bundle utilizing DS0s 1-3 and 8-10 of T1 number 3.

Configure a Fractional T1 HDLC Bundle

```
Blackbox/configure> interface bundle demo1
Blackbox/configure/interface/bundle> link t1 3:1-3,8-10
Blackbox/configure/interface/bundle> encap hdlc
Blackbox/configure/interface/bundle> ip addr 10.1.1.1 255.255.255.252
Blackbox/configure/interface/bundle> exit
```

27.1.3 T1

The following example creates a 1536 Kbps T1 bundle utilizing T1 number 4. This bundle uses IP unnumbered.

Configure a T1 PPP Bundle

```
Blackbox/configure> interface bundle demo2
Blackbox/configure/interface/bundle> link t1 4
Blackbox/configure/interface/bundle> encap ppp
Blackbox/configure/interface/bundle> ip unnumbered ethernet0
Blackbox/configure/interface/bundle> exit
```

27.1.4 NxT1

The following example creates a 4.5 Mbps N x T1 bundle utilizing T1s 6-8. MLPPP is not explicitly specified, a PPP bundle with two or more linked T1s uses the multi-link protocol by definition.

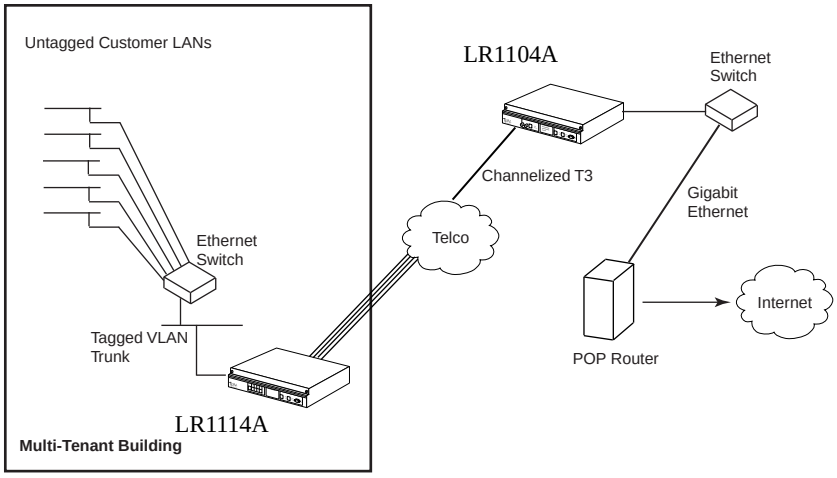
Configure an N x T1 MLPPP Bundle

```
Blackbox/configure> interface bundle demo3
Blackbox/configure/interface/bundle> link t1 6-8
Blackbox/configure/interface/bundle> encap ppp
Blackbox/configure/interface/bundle> ip addr 10.1.1.5 255.255.255.252
Blackbox/configure/interface/bundle> exit
```

26
VIRTUAL LAN FORWARDING

26.1 Managing VLAN Traffic

Figure 43 VLAN Forwarding: Multi-Tenant Internet Access



The example above shows each multi-tenant customer represented as a separate VLAN on the Ethernet switch. The connection in the customer office can be routed or bridged, depending on whether the provider will be hosting customer applications at the POP. The Ethernet switch passes a VLAN trunk to the Black Box LR1114A that forwards traffic, based on the VLAN tags, from this interface to the multilink bundle.

At the POP, tagged traffic is forwarded to a VLAN trunk port on the Ethernet switch. Routing between customer VLANs is provided by the POP router using sub-interfaces on the Gigabit Ethernet VLAN trunk. The customer LAN subnet is extended all the way to the POP router making remote management of LAN services (e.g., DHCP, file servers. SMTP) possible.

The VLAN forwarding feature has the added benefit of being able to support non-IP traffic since all traffic is forwarded based only on the Layer 2 VLAN tag. Although Black Box products do not communicate using non-IP Layer 3 protocols, Black Box systems can forward these protocols.

The management VLAN feature provides in-band communication with the Black Box systems as well as the Ethernet switches while remaining separate from customer traffic. The Black Box systems will examine the destination IP address of any packets received on the management VLAN. If the destination is the Black Box, the address of the

packet will be forwarded to the IP layer for local processing. If the address does not match the address of the Black Box system, the packet will be forwarded to all interfaces configured for the management VLAN with the exception of the interface where it was received. This allows all transmission equipment to be managed in a single, flat VLAN.

When the Black Box system generates traffic on to the management VLAN, an ARP request is generated in the direction of the VLAN's default route. If no default is configured, the ARP request will be generated in all possible directions, and the interface receiving the response will be cached with the reply. The source MAC address used by the Black Box will be associated with the Ethernet port associated with the management VLAN.

In a multi-tenant unit (MTU) where customer Internet access is through the Ethernet interface, some form of bandwidth control is necessary to prevent a high bandwidth customer from blocking others since the uplink out of the building will typically be less than 10 Mbps. Black Box provides QoS support to limit customer bandwidth using a committed rate and burst rate, ensuring that customers get consistent bandwidth performance as other customers are activated. Black Box's QoS can be configured based on VLAN IDs, in increments of 64 kbps providing greater control than what is normally available in Ethernet switches.

26.1.1POP configuration: Black Box LR1104A

```
LR1104A/configure> hostname POP-LR1104A
POP-LR1104A/configure> no ftp_server
POP-LR1104A/configure> no autoconf
```

26.1.1.1 Configure mlppp bundle interface

```
POP-LR1104A/configure> interface bundle bldg1
POP-LR1104A/configure/interface/bundle bldg1> link ct3 1 1-4
POP-LR1104A/configure/interface/bundle bldg1> encapsulation ppp
POP-LR1104A/configure/interface/bundle bldg1> ip unnumbered ethernet0
POP-LR1104A/configure/interface/bundle bldg1> exit
```

26.1.1.2 Configure interface ethernet 0

```
POP-LR1104A/configure> interface ethernet 0
POP-LR1104A/configure/interface/ethernet0> speed 100 full_duplex
POP-LR1104A/configure/interface/ethernet0> ip address 10.1.1.2 255.255.255.0
POP-LR1104A/configure/interface/ethernet0> exit
```

26.1.1.3 Configure in-band vlan forwarding table

```
POP-LR1104A/configure> vlanfwd
POP-LR1104A/configure/vlanfwd > add vlanid 4092 ethernet0
POP-LR1104A/configure/vlanfwd > add vlanid 4092 bldg1
POP-LR1104A/configure/vlanfwd > add vlanid 11-18 ethernet0
POP-LR1104A/configure/vlanfwd > add vlanid 11-18 bldg1
POP-LR1104A/configure/vlanfwd > management
POP-LR1104A/configure/vlanfwd/management> vlanid 4092
POP-LR1104A/configure/vlanfwd/management> disable_ipfwd
POP-LR1104A/configure/vlanfwd/management> default_route 10.1.1.1 ethernet0
POP-LR1104A/configure/vlanfwd/management> exit 2
```

26.1.1.4 Configure rate limiting for vlans

```
POP-LR1104A/configure> interface bundle bldg1
POP-LR1104A/configure/interface bundle bldg1> no enable_cbq
POP-LR1104A/configure/interface bundle bldg1> add_class mgmt-vlan root-out vlan_id 4092 cr 10
be 3072
POP-LR1104A/configure/interface bundle bldg1> add_class custA root-out vlan_id 11 cr 128 br
1024
POP-LR1104A/configure/interface bundle bldg1> add_class custB root-out vlan_id 12 cr 128 br
1024
POP-LR1104A/configure/interface bundle bldg1> add_class custC root-out vlan_id 13 cr 128 br
1024
POP-LR1104A/configure/interface bundle bldg1> add_class custD root-out vlan_id 14 cr 128 br
1024
POP-LR1104A/configure/interface bundle bldg1> add_class custE root-out vlan_id 15 cr 128 br
1024
POP-LR1104A/configure/interface bundle bldg1> add_class custF root-out vlan_id 16 cr 128 br
1024
POP-LR1104A/configure/interface bundle bldg1> add_class custG root-out vlan_id 17 cr 128 br
1024
POP-LR1104A/configure/interface bundle bldg1> add_class custH root-out vlan_id 18 cr 128 br
1024
POP-LR1104A/configure/interface bundle bldg1> enable_cbq
POP-LR1104A/configure/interface bundle bldg1> exit
```

26.1.2Bldg1 configuration: Black Box LR1114A

```
LR1114A/configure> hostname bldg1-LR1114A
bldg1-LR1114A/configure> interface ethernet 0
bldg1-LR1114A/configure/interface/ethernet0 > ip addr 10.1.1.3 255.255.255.0
bldg1-LR1114A/configure> interface ethernet0> exit
```

26.1.2.1 Configure interface bundle uplink

```
bldg1-LR1114A/configure> interface bundle uplink
bldg1-LR1114A/configure/interface/bundle uplink> link t1 1-4
bldg1-LR1114A/configure/interface/bundle uplink> encapsulation ppp
bldg1-LR1114A/configure/interface/bundle uplink> ip unnumbered ethernet0
bldg1-LR1114A/configure/interface/bundle uplink> exit
```

26.1.2.2 Configure inband VLAN forwarding table

```
bldg1-LR1114A/configure/interface> vlanfwd
bldg1-LR1114A/configure/interface/vlanfwd> add vlanid 4092 ethernet0
bldg1-LR1114A/configure/interface/vlanfwd> add vlanid 4092 uplink
bldg1-LR1114A/configure/interface/vlanfwd> add vlanid 11-18 ethernet0
bldg1-LR1114A/configure/interface/vlanfwd> add vlanid 11-18 uplink
bldg1-LR1114A/configure/interface/vlanfwd> management
bldg1-LR1114A/configure/interface/vlanfwd/management> vlanid 4092
bldg1-LR1114A/configure/interface/vlanfwd> disable_ipfwd
bldg1-LR1114A/configure/interface/vlanfwd> default_route 10.1.1.1 uplink
bldg1-LR1114A/configure/interface/vlanfwd> exit 2
```

26.1.2.3 Configure rate limiting for VLANs

```
bldg1-LR1114A/configure> interface bundle uplink
bldg1-LR1114A/configure/interface/bundle uplink> qos
bldg1-LR1114A/configure/interface/bundle uplink> no enable_cbq
bldg1-LR1114A/configure/interface/bundle uplink> add_class mgmt-vlan root-out vlan_id 4092 cr
10 br 3072
bldg1-LR1114A/configure/interface/bundle uplink> add_class custA root-out vlan_id 11 cr 128 br
1024
bldg1-LR1114A/configure/interface/bundle uplink> add_class custB root-out vlan_id 12 cr 128 br
1024
bldg1-LR1114A/configure/interface/bundle uplink> add_class custC root-out vlan_id 13 cr 128 br
1024
bldg1-LR1114A/configure/interface/bundle uplink> add_class custD root-out vlan_id 14 cr 128 br
1024
bldg1-LR1114A/configure/interface/bundle uplink> add_class custE root-out vlan_id 15 cr 128 br
1024
bldg1-LR1114A/configure/interface/bundle uplink> add_class custF root-out vlan_id 16 cr 128 br
1024
bldg1-LR1114A/configure/interface/bundle uplink> add_class custG root-out vlan_id 17 cr 128 br
1024
bldg1-LR1114A/configure/interface/bundle uplink> add_class custH root-out vlan_id 18 cr 128 br
1024
bldg1-LR1114A/configure/interface/bundle uplink> enable_cbq
bldg1-LR1114A/configure/interface/bundle uplink> exit
```

26.1.2.4 Configure SNMP

```
bldg1-LR1114A/configure> snmp
bldg1-LR1114A/configure/snmp> community public ro
bldg1-LR1114A/configure/snmp> system_id bldg1-LR1114A
bldg1-LR1114A/configure/snmp> trap_host 10.2.1.1 public
bldg1-LR1114A/configure/snmp> exit
```

27
MUTLILINK FRAME RELAY

27.1Multilink Frame Relay FRF.15 and FRF.16

Multilink Frame Relay (MFR) is actually composed of two standards: FRF.15 and FRF.16. The latter is more common and defines UNI/NNI interfaces for implementing MFR. FRF.16 is used for multiplexing dedicated T1s in the local loop and requires compatible equipment at the carrier POP. FRF.15, or DTE-to-DTE MFR is used for multiplexing frame relay T1s between end points without impacting POP equipment. As a result, FRF.15 can be implemented across multiple frame relay carriers to provide additional redundancy. This application discusses considerations for using this standard. All Black Box products support FRF.15 and FRF.16.

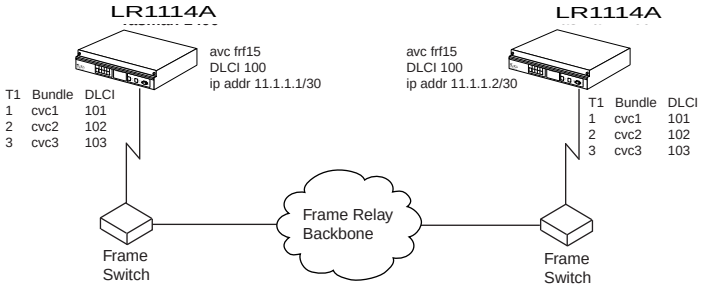
27.1.1 Features

- Low cost way of providing added bandwidth to private networks
- Can be done without the knowledge of the Frame Relay provider
- Scalable bandwidth using MFR for customers based on T1 access
- Traffic can be routed or switched using Frame Relay at the end points

A customer desiring to implement DTE-to-DTE MFR can use the architecture illustrated in Figure 1. The normal ordering process can be used to obtain the fame relay T1s. From the perspective of the CPE, the Black Box LR1114As combine those different frame relay PVCs into a consolidated, larger pipe.

FRF.15 uses an aggregated virtual circuit (AVC) for the combined interface. The AVC is composed of constituent virtual circuits (CVC) that represent the frame relay T1s ordered from the carrier(s). In this example, the Black Box LR1114As are configured with DTE LMI; the carrier frame switches are DCE.

Figure 44 MFR Using FRF.15



In Black Box systems, CVCs are configured using the *bundle* construct normally used for a non-ethernet interface. After the CVCs are configured, they can be assigned to the AVC. The AVC, frf15 in this case, is assigned a DLCI of 100 on both ends and an IP address in the 11.1.1.0/30 subnet. The AVC names and DLCI numbers can be different on

each end if necessary. The frame switches are configured for DLCIs 101, 102, and 103 on the respective T1s. In this example, the Black Box LR1114A configurations are almost identical. The primary difference is the IP address assigned to the AVC. The configuration for the left LR1114A is shown below.

27.1.1.1 # Configure Ethernet interface

```
Blackbox/configure> interface ethernet 0
Blackbox/configure/ethernet0> ip addr 192.168.1.1 255.255.255.0
Blackbox/configure/ethernet0> exit
```

27.1.1.2 # Configure CVC1

```
Blackbox/configure> interface bundle cvc1
Blackbox/configure/interface/bundle cvc1> link t1 1
Blackbox/configure/interface/bundle cvc1> encapsulation frelay
Blackbox/configure/interface/bundle cvc1> fr
Blackbox/configure/interface/bundle cvc1/fr> intf_type dte
Blackbox/configure/interface/bundle cvc1/fr> pvc 101
Blackbox/configure/interface/bundle cvc1/fr> exit 3
```

27.1.1.3 # Congfigure CVC2

```
Blackbox/configure> interface bundle cvc2
Blackbox/configure/interface/bundle cvc2> link t1 2
Blackbox/configure/interface/bundle cvc2> encapsulation frelay
Blackbox/configure/interface/bundle cvc2> fr
Blackbox/configure/interface/bundle cvc2/fr> intf_type dte
Blackbox/configure/interface/bundle cvc2/fr> pvc 102
Blackbox/configure/interface/bundle cvc2/fr> exit 3
```

27.1.1.4 # Configure CVC3

```
Blackbox/configure> interface bundle cvc3
Blackbox/configure/interface/bundle cvc3> link t1 2
Blackbox/configure/interface/bundle cvc3> encapsulation frelay
Blackbox/configure/interface/bundle cvc3> fr
Blackbox/configure/interface/bundle cvc3/fr> intf_type dte
Blackbox/configure/interface/bundle cvc3/fr> pvc 103
Blackbox/configure/interface/bundle cvc3/fr> exit 3
```

27.1.1.5 #Configure AVC

```
Blackbox/configure> interface avc frf15 100
Blackbox/configure/interface/avc frf15 100> cvc 101 cvc1
Blackbox/configure/interface/avc frf15 100> cvc 102 cvc2
Blackbox/configure/interface/avc frf15 100> cvc 103 cvc 3
Blackbox/configure/interface/avc frf15 100> ip address 11.1.1.1 255.255.255.252
Blackbox/configure/interface/avc frf15 100> exit
Blackbox> configure
```

The above configuration does not include statements for policing and traffic shaping, so all PVCs are given the full CIR for the interface. Once the AVC is configured, the Black Box systems can be configured for transparent IP multiplexing or for static routing. These details are omitted.

The primary advantage of FRF.15 is that no support is required on the POP side of the network. That fact makes this standard ideal for companies that need increased bandwidth for their frame relay based private network. FRF.15 is more susceptible to differential delay because the multiplexed links extend well beyond the local loop. Fortunately, differential delay encountered within the United States is typically small enough to have little to no impact on actual traffic flow.

28

CONFIGURING FRAME RELAY AND MULTILINK FRAME RELAY

28.1 Layer Two Configurations FR and MFR

Figure 45 outlines a Multilink Frame Relay (MFR) configuration with three sites. PVC 16 connects Site 1 to Site 3, while PVC 31 connects Site 2 to Site 3. The Frame Relay switching equipment is represented simply as a Frame cloud.

Figure 45 MFT Configuration

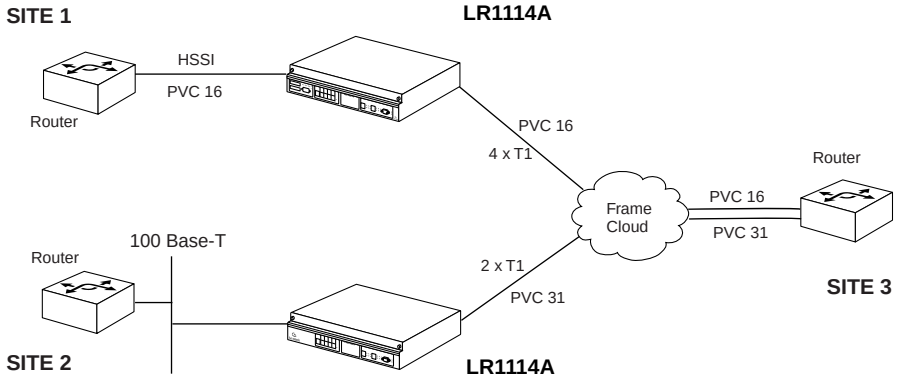
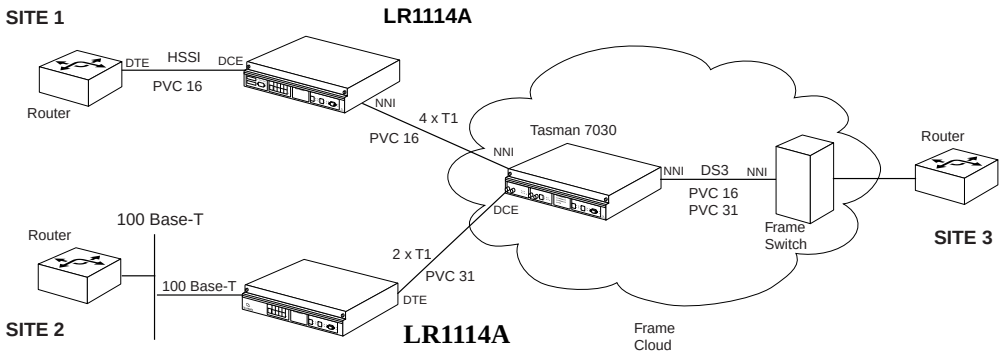


Figure 46 provides greater detail, including the use of a LR1104A inside the cloud as a Frame Relay switching device, and LR1114A series units at the CPE sites 1 and 2.

Figure 46 MFR Configuration Detail



28.1.1 FR Configuration

A LR1104A LR1104A at Site 1 provides Frame Relay switching between a HSSI interface, connecting to the local router, and a 4 x T1 MFR bundle, connecting to the LR1104A. Continuity of PVC 16 is maintained through the LR1104A LR1104A, though this is not required.

The HSSI connection between the router and the LR1104A is defined as type UNI. The LR1104A serves as Frame Relay DCE and the router as the Frame Relay DTE. Note that the Frame Relay (Layer 2) interface type is independent of, and not necessarily the same as, the HSSI (Layer 1) interface type.

28.1.1.1 Configure the HSSI Bundle at Site 1

```
Blackbox/configure> interface bundle toRouter
Blackbox/configure/interface/bundle> link ussi 1
Blackbox/configure/interface/bundle> description "hssi link to router"
Blackbox/configure/interface/bundle> encap fr
Blackbox/configure/interface/bundle> fr
Blackbox/configure/interface/bundle/fr> intf_type dce
Blackbox/configure/interface/bundle/fr> lmi ansi
Blackbox/configure/interface/bundle/fr/lmi> exit
Blackbox/configure/interface/bundle/fr> pvc 16
/* pvc's default cir set to 52000000 bps */
Blackbox/configure/interface/bundle/fr/pvc> shaping cir 6144000 bcmax 6144000 bcmin
3072000
Blackbox/configure/interface/bundle/fr/pvc> exit
```

The BlackBox serves as a Frame Relay switch, connecting PVCs 16 and 31 through to another Frame Switch via a Clear Channel DS-3 interface. Note that the Bcmin setting of 3.072 Mbps is maintained across all PVC 16 configurations, to correspond to the Class C setting of the MFR portion of the PVC.

28.1.1.2 Configure the Clear Channel Bundle on the LR1104A

```
Blackbox/configure> int bundle toFRSwit
Blackbox/configure/interface/bundle> link t3 1
Blackbox/configure/interface/bundle> description "DS-3 bundle to FR Switch"
Blackbox/configure/interface/bundle> encap fr
Blackbox/configure/interface/bundle> fr
Blackbox/configure/interface/bundle/fr> intf_type nni
Blackbox/configure/interface/bundle/fr> lmi ansi
Blackbox/configure/interface/bundle/fr/lmi> exit

Blackbox/configure/interface/bundle/fr> pvc 16
Blackbox/configure/interface/bundle/fr/pvc> shaping cir 6144000 bcmax 6144000 bcmin 3072000
Blackbox/configure/interface/bundle/fr/pvc> switch 16 toBlackBox
Blackbox/configure/interface/bundle/fr/pvc> exit

Blackbox/configure/interface/bundle/fr> pvc 31
Blackbox/configure/interface/bundle/fr/pvc> shaping cir 3072000 bcmax 3072000 bcmin 1536000
Blackbox/configure/interface/bundle/fr/pvc> switch 31 toLR1114A
```

28.1.2 MFR Configuration

The 4 x T1 MFR bundle between the LR1104A and the Black Box connects two Frame Relay switches, therefore it represents an NNI interface. The sample configuration defines the 4 x T1 bundle to be of Class C; that is, a minimum of 2 T1 links are required to be up in order to keep the bundle up. Settings for Bcmin on the MFR bundle are set to correspond with the Class C configuration; that is, the minimum anticipated bandwidth will be 2 x T1.

28.1.2.1 Configure the LR1104A LR1104A at Site 1

```
Blackbox/configure> int bundle wan1
Blackbox/configure/interface/bundle> link t1 5-8
Blackbox/configure/interface/bundle> description "6 Mbps MFR"
Blackbox/configure/interface/bundle> encap fr
Blackbox/configure/interface/bundle> fr
Blackbox/configure/interface/bundle/fr> intf_type nni
Blackbox/configure/interface/bundle/fr> mfr class C 2
/* specifies that the bundle remain up as long as two T1s are up */
Blackbox/configure/interface/bundle/fr> lmi ansi
Blackbox/configure/interface/bundle/fr/lmi> keepalive 8
Blackbox/configure/interface/bundle/fr/lmi> exit
Blackbox/configure/interface/bundle/fr> pvc 16
/* pvc's default cir set to 6144000 bps */
Blackbox/configure/interface/bundle/fr/pvc> shaping cir 6144000 bcmax 6144000 bcmin 3072000
/* Bcmin consistent with minimum possible bundle bandwidth of two T1s */
Blackbox/configure/interface/bundle/fr/pvc> switch 16 toRouter
/* switch between wan1:16 and toRouter:16 established */
Blackbox/configure/interface/bundle/fr> exit
```

28.1.2.2 Configure the LR1104A

```
Blackbox/configure> int bundle toBlackBox
Blackbox/configure/interface/bundle> link ct3 1 1-4
Blackbox/configure/interface/bundle> description "6Mbps MFR to LR1104A"
Blackbox/configure/interface/bundle> encap fr
Blackbox/configure/interface/bundle> fr
Blackbox/configure/interface/bundle/fr> intf_type nni
Blackbox/configure/interface/bundle/fr> mfr class C 2
Blackbox/configure/interface/bundle/fr> lmi ansi
Blackbox/configure/interface/bundle/fr/lmi> keepalive 10
Blackbox/configure/interface/bundle/fr/lmi> exit
Blackbox/configure/interface/bundle/fr> pvc 16
Blackbox/configure/interface/bundle/fr/pvc> shaping cir 6144000 bcmax 6144000 bcmin 3072000
Blackbox/configure/interface/bundle/fr/pvc> exit
Blackbox/configure/interface/bundle/fr> exit 2
```

A LR1104A LR1114A at Site 2 serves as the Frame Relay termination point, connecting the Site 2 IP network to the LR1104A. This MFR bundle utilizes 2 T1 links for an approximate 3 Mbps bandwidth. Since it is the Frame Relay terminating point and is defined as a DTE frame relay interface, an IP address is assigned to the WAN bundle.

28.1.2.3 Configure the LR1104A LR1114A at Site 2

LR1114A/configure> **int bundle frame1**
LR1114A/configure/interface/bundle> **link t1 1-2**
LR1114A/configure/interface/bundle> **description "3 Mbps to the Internet"**
LR1114A/configure/interface/bundle> **encap fr**
LR1114A/configure/interface/bundle> **fr**
LR1114A/configure/interface/bundle/fr> **intf_type dte** /* this is default */
LR1114A/configure/interface/bundle/fr> **mfr class A** /* this is default */
LR1114A/configure/interface/bundle/fr> **lmi ansi**
LR1114A/configure/interface/bundle/fr/lmi> **keepalive 10**
LR1114A/configure/interface/bundle/fr/lmi> **exit**
LR1114A/configure/interface/bundle/fr> **pvc 31**
/* pvc's default cir set to 3072000 bps */
LR1114A/configure/interface/bundle/fr/pvc> **ip addr 10.0.2.1 255.255.255.252**
LR1114A/configure/interface/bundle/fr/pvc> **enable**
LR1114A/configure/interface/bundle/fr/pvc> **exit**

28.1.2.4 Configure the LR1104A

Blackbox/configure> **int bundle toLR1114A**
Blackbox/configure/interface/bundle> **link ct3 1 5-6**
Blackbox/configure/interface/bundle> **description "3Mbps MFR to LR1114A"**
Blackbox/configure/interface/bundle> **encap fr**
Blackbox/configure/interface/bundle> **fr**
Blackbox/configure/interface/bundle/fr> **intf_type dce**
Blackbox/configure/interface/bundle/fr> **lmi ansi**
Blackbox/configure/interface/bundle/fr/lmi> **keepalive 10**
Blackbox/configure/interface/bundle/fr/lmi> **exit**
Blackbox/configure/interface/bundle/fr> **pvc 31**
Blackbox/configure/interface/bundle/fr/pvc> **exit 3**

1000 Park Drive • Lawrence, PA 15055-1018 • 724-746-5500 • Fax 724-746-0746