IP Reassembly for Tunnels 5

This chapter describes IP packet reassembly for tunneled protocols on the ERX system.

Overview

Tunneling protocols provide a method of forwarding packets of a particular protocol through a network of a different protocol type. For example, L2TP can transport a protocol such as PPP through a routed IP network. This capability requires a pair of devices that define the endpoints of the tunnel. Packets entering the tunnel are processed and encapsulated at the ingress endpoint, and packets exiting the tunnel are processed and decapsulated at the egress endpoint.

When packets are tunneled through an IP network, simple IP forwarding is performed. The IP forwarding process may require fragmentation within the tunnel, which means that a packet that enters a tunnel whole may reach the egress endpoint as fragments. Because tunnel processing requires each packet to exit the tunnel in the same form in which it entered, if fragmented packets are not reassembled before the tunnel egress processing is performed, they are dropped.

For example, in Figure 5-1, traffic is tunneled through an IP network that has four hops. Because the MTU of the link between routers B and C is smaller than that of previous hops, some packets are fragmented. Router

D must reassemble the packets before tunnel egress processing and decapsulation are performed.

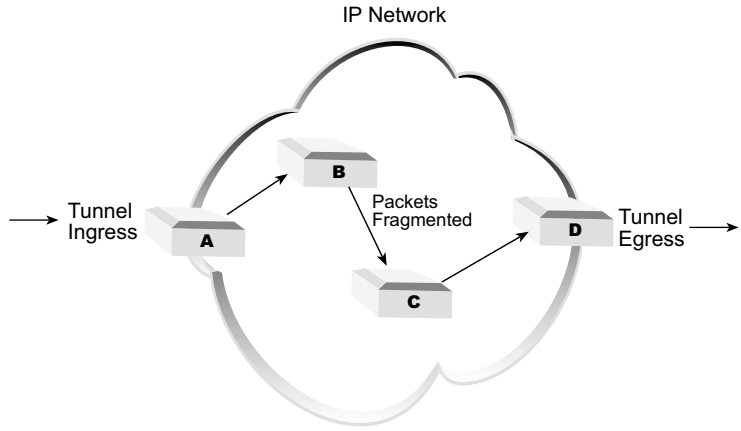

Figure 5-1 Tunneling through an IP network that fragments packets

Reassembly Processing Within the System

Tunnel Server modules (TSMs) perform IP reassembly on the ERX system. The ERX system can perform reassembly of IP packets it receives on DVMRP, GRE, IPSec, L2F, and L2TP tunnels.

Because IP reassembly is required only on tunnel egress packets, the system performs reassembly only on packets in which the IP destination address is local to the router and in which the underlying protocol is one of the supported tunneling protocols.

Configuring IP Reassembly

To set up IP reassembly, you enable it on a virtual router basis. Also, on a system-wide basis, you can control how the system handles checking of sequence numbers in data packets that it receives on L2TP and L2F tunnels.

ip tunnel reassembly

- Use to enable the reassembly of fragmented IP tunnel packets that are received on the current virtual router.
- Note that you configure tunnel reassembly on VPN routing and forwarding routers independent of the tunnel reassembly configuration on the parent virtual router.

- Example – enables reassembly for virtual router vr12 and disables reassembly for virtual router vr8

```
host1:vr12(config)#ip tunnel reassembly
host1:vr12(config)#virtual-router vr8
host1:vr8(config)#no ip tunnel reassembly
```

- Use the **no** version to return IP tunnel reassembly to the default, disabled.

l2f ignore-receive-data-sequencing

- Use to prevent sequence number checking for data packets received on all L2F tunnels in the system. This command does not affect the insertion of sequence numbers in packets sent from the system.
- It is recommended that you set up the system to ignore sequence numbers in received data packets if you are using IP reassembly. Because IP reassembly may reorder L2F packets, out-of-order packets may be dropped if sequence numbers are being used on L2F data packets.
- Example

```
host1(config)#l2f ignore-receive-data-sequencing
```

- Use the **no** version to cause the system to check sequence numbers on received L2F data packets.

l2tp ignore-receive-data-sequencing

- Use to prevent sequence number checking for data packets received on all L2TP tunnels in the system. This command does not affect the insertion of sequence numbers in packets sent from the system.
- It is recommended that you set up the system to ignore sequence numbers in received data packets if you are using IP reassembly. Because IP reassembly may reorder L2TP packets, out-of-order packets may be dropped if sequence numbers are being used on L2TP data packets.
- Example

```
host1(config)#l2tp ignore-receive-data-sequencing
```

- Use the **no** version to cause the system to check sequence numbers on received L2TP data packets.

Monitoring IP Reassembly

The system keeps several statistics that are useful for diagnostic purposes. These statistics are organized by virtual router, and some are broken out by protocol as well. You can display statistics for a single virtual router or for all virtual routers.

show ip tunnel reassembly statistics

- Use to display reassembly statistics.
- Statistics are displayed for the current virtual router unless you include the **all** keyword, which causes the system to display statistics for all virtual routers.
- Statistics are displayed in brief form unless you include the **detail** keyword.
- Field descriptions
  - Tunnel IP reassembly – status of the IP reassembly feature: enabled, disabled
  - Fragments Received – total fragments received for all tunneling protocols
  - Packets Reassembled – number of packets reassembled; detailed display includes number of packets reassembled for each protocol
  - Reassembly Errors – errors in completing reassembly; detailed display includes types of reassembly errors
  - Reassembly Discards – number of packets discarded because they were not reassembled; detailed displays include the cause of discard
- Example 1 – show reassembly statistics for all virtual routers

```
host1:vr0#show ip tunnel reassembly statistics all
IP Reassembly Statistics for Virtual Router: vr0
      Tunnel IP reassembly enabled
      Fragments Received: 2685
      Packets Reassembled: 1231
      Reassembly Errors: 22
      Reassembly Discards: 1422
      Fabric Drops: 10
IP Reassembly Statistics for Virtual Router: vr1
      Tunnel IP reassembly disabled
      Fragments Received: 3031
      Packets Reassembled: 0
      Reassembly Errors: 0
      Reassembly Discards: 3031
      Fabric Drops: 0
IP Reassembly Statistics for Virtual Router: vr2
      Tunnel IP Reassembly enabled
      Fragments Received: 0
      Packets Reassembled: 0
      Reassembly Errors: 0
      Reassembly Discards: 0
```

› Example 2 – shows detailed reassembly statistics for virtual router vr0

```
host1:vr0#show ip tunnel reassembly statistics detail
IP Reassembly Statistics for Virtual Router: vr0
      Tunnel IP Reassembly enabled
      Fragments Received: 2685
Packets Reassembled: 1231
            L2TP: 348
            L2F:    0
            GRE:  883
            IPSec:  0
Reassembly Errors: 22
            Fragmentation errors: 0
            Too many fragments:   0
            Out of resources:     0
            Packet too big:       0
            Reassembly Timeouts: 22
Reassembly Discards: 1422
            L2TP reassembly disabled: 0
            L2F reassembly disabled:  1422
            GRE reassembly disabled:  0
            IPSec reassembly disabled: 0
            Virtual router reassembly disabled: 0
```