7.5.3 Troubleshooting Routing Facts

A general routing problem symptom is the inability to access hosts on a specific network or any remote network. The following table lists various problems that are typically caused by routing issues:

Problem	Description
Can't access hosts outside the local subnet	If one or more hosts can communicate only with hosts on the local subnet, the problem is likely with the default gateway configuration. • If a single host is having problems, check the default gateway setting on that host. • If multiple hosts are having problems, check the default gateway setting, and verify that the DHCP server is configured to deliver the correct default gateway address. • If all hosts have the same problem and the default gateway setting is correct, verify that the default gateway server is up and configured for routing. This issue could also be caused by problems with the Neighbor Discovery (ND) protocol. • Routers on the same link use the ND protocol to advertise their existence to neighboring routers and to learn about the existence of their neighbors. • Routers process ND messages to identify the link layer addresses of neighboring devices that are directly connected to the router. • Routers use the ND protocol to periodically send and receive small hello packets to and from neighboring routers. If hello packets are not received from a particular router, that router is assumed to be not functioning. Issues with the ND protocol can occur when a large subnet is used for point-to-point links between routers, especially when IPv6 is used. By convention, a /64 prefix is used on each subnet when implementing IPv6, allowing for a very large number of hosts on the subnet. If you use a standard /64 prefix on the link subnet, the ND protocol will try to perform address resolution for all possible hosts on the subnet. When this happens, newly connected devices may not be recognized by other routers for a long period of time. A point-to-point link between routers is composed of only two interfaces, one on each end of the link. Therefore, the link subnet needs only to support a maximum of two hosts. As a recommended best practice, use a very small subnet for the point-to-point link between routers to reduce ND traffic. The recommendation is to use 127-bit (/127) prefixes on these links instead of the conventional 64-bit prefix.

Can't communicate with any host on a specific network	If hosts are unable to contact hosts on a specific subnet, but they can communicate with other subnets, try the following:
	
	• Verify that the router connected to the subnet is up.
	• Use the **route** command on the default gateway of the local subnet and verify that the router has a route to the remote subnet. If necessary, configure a routing protocol so that the route can be learned automatically, or configure a static route.
	• Use **traceroute** to view the route taken to the destination network. Identify the last router in the path, then troubleshoot routing at that point.
	• Check for routing loops in the path to the destination network. A routing loop is caused by a misconfiguration in the routers along the path, causing data to be sent back along the same path rather than forwarded to the destination. Routing loops are indicated by:
	    • Routing table entries that appear and then disappear (called *route flapping*), often at regular intervals (such as every minute).
	    • Routing table entries where the next hop router address oscillates (switches) between two or more different routers.
	
	        Routing loops are displayed in a **traceroute** output and shows the same sequence of routers being repeated.
	
	• Check for black hole routers. A *black hole router* will drop packets when the packet size exceeds the Maximum Transmission Unit (MTU) size. You can use **ping** to locate a black hole router by setting the following parameters along with the IP address of the remote host:
	    • **-f** causes the ping utility to send an ICMP echo packet that has the IP "Do not Fragment" or DF bit set.
	    • **-l** sets the buffer (or payload) size of the ICMP echo packet. Specify this size by typing a number after the **-l** parameter.
	
	The ping test will provide you with helpful information:
	    • If the MTU of every segment of a routed connection is at least the MTU size, the packet is successfully returned.
	    • If there are intermediate segments that have smaller MTUs, and the routers return the appropriate ICMP "destination unreachable" packet, the ping utility displays the message, "Packet needs to be fragmented but DF set."
	    • If there are intermediate segments that have smaller MTUs, and the routers do not return the appropriate

	ICMP "destination unreachable" packet, the ping utility displays the message, "Request timed out."
Can't access the Internet	If hosts are able to reach all internal networks but can't access the Internet, try the following: • Verify that the Internet connection is up. • Check for a default route on the router connected to the Internet. A default route is indicated by a network address of 0.0.0.0 with a mask of 0.0.0.0. The default route is used for packets that do not match any other entries in the routing table. Most routers that connect private networks to the Internet do not know about specific networks and routes on the Internet. Additionally, most routers do not share routes for private subnets with Internet routers. A router is configured with a single default route that is used for all Internet traffic, and a router at the ISP is responsible for sharing a single route for your private network with other Internet routers.
Remote clients can't access network resources	If you have remote access clients who can establish a connection to the remote access server but can't connect to other resources on the private network, check the following: • If remote clients are being assigned IP addresses on the same subnet as the private network, make sure that proxy ARP is enabled on the LAN interface of the remote access server. Proxy ARP makes it appear as if the remote clients are connected to the same network segment. • If remote clients are being assigned IP addresses on a different subnet than the private network, make sure the remote access server is configured to route packets between the remote clients and the private network.