

“Routing table cannot be altered” message

In some situations the “The routing table cannot be altered after the Extranet Connection has been established.... The Extranet Connection has been Closed” message might appear on the client’s machine followed by the tunnel tear down.

This error message was intended to appear on the client’s machine when changes to the routing table are made on the client’s machine. Changing the routing table poses a potential risk of bypassing the policy passed by Contivity* to the client, this in turn leads to a potential security risk by allowing an unauthorized access. So when Contivity detects the routing table change and, therefore, the violation of the security policy, Contivity drops the tunnel connection to stop the intrusion.

The possible causes for the routing table changes are as follows:

1. Client’s machine has several NIC cards, the tunnel is through one of them and when there are any changes to the other cards (for example, interface goes down) the change to the routing table is made.
2. Client has a short lease time for the IP address acquired through the DHCP, table changes after the address renewal/acquisition (if IP changes).
3. Some applications on the client’s machine rewrite the routing table (for example, issuing the **route add** command).
4. Routing updates from dynamic protocols like RIP or OSPF change the table.
5. ICMP redirect messages have been received by the client’s machine.
6. Internet connection sharing.

The routing table check security feature was first introduced in the Extranet Access Client (EAC) code version 2_62.47. All versions prior to this release didn’t have the routing table check and, therefore, are considered to be less secure.

With the introduction of the filter driver, there is no longer a need to check the routing table when client/Contivity are not operating in the split tunneling mode. Since filter driver now only allows the traffic to leave/enter the system that has originated from the Contivity and is destined for the client (or vice versa). This change was introduced in the V04_65_019 Contivity VPN client code version and will be incorporated in all the future releases.

The routing table check still applies to the operation in the split-tunneling mode to ensure the security of the client/server session.

To avoid the “Routing table cannot be altered” message, make sure nothing changes the routing table while the secure tunnel connection is established between VPN client and the Contivity.

“Routing table cannot be altered” message

Copyright 2003, Nortel Networks. All rights reserved.

*Nortel Networks, the Nortel Networks logo, the Globemark, Unified Networks, and Contivity are trademarks of Nortel Networks.

Information in this document is subject to change without notice. Nortel Networks assumes no responsibility for errors that might appear in this document.

If you found this document useful and would like to see more similar documents please send your feedback to CRCONT@nortelnetworks.com with the subject heading "How To Documentation."

If after following this guide you are still having problems please ensure you have carried out the steps exactly as in this document. You should also check the Nortel Networks [FAQs/Solutions Search Knowledge Database](#) for additional help. If problems still persist, please contact Nortel Networks Customer Support.

Author: Kristina Senkova kristise@nortelnetworks.com

Technical Support Contact Information:

Nortel Networks is committed to bettering the customer experience through its Customer TouchPoint Program (CTP) – where in most countries one number can be used to contact Nortel Networks. To obtain regional telephone contact information, please visit the following web site: <http://www.nortelnetworks.com/help/contact/global/>.