Configuration of VPN Tunnel between DX Series Routers

Belden, Belden Sending All The Right Signals, Hirschmann, GarrettCom, Tofino Security, Lumberg Automation and the Belden logo are trademarks or registered trademarks of Belden Inc. or its affiliated companies in the United States and other jurisdictions. Belden and other parties may also have trademark rights in other terms used herein.

Contents

Featured Brands

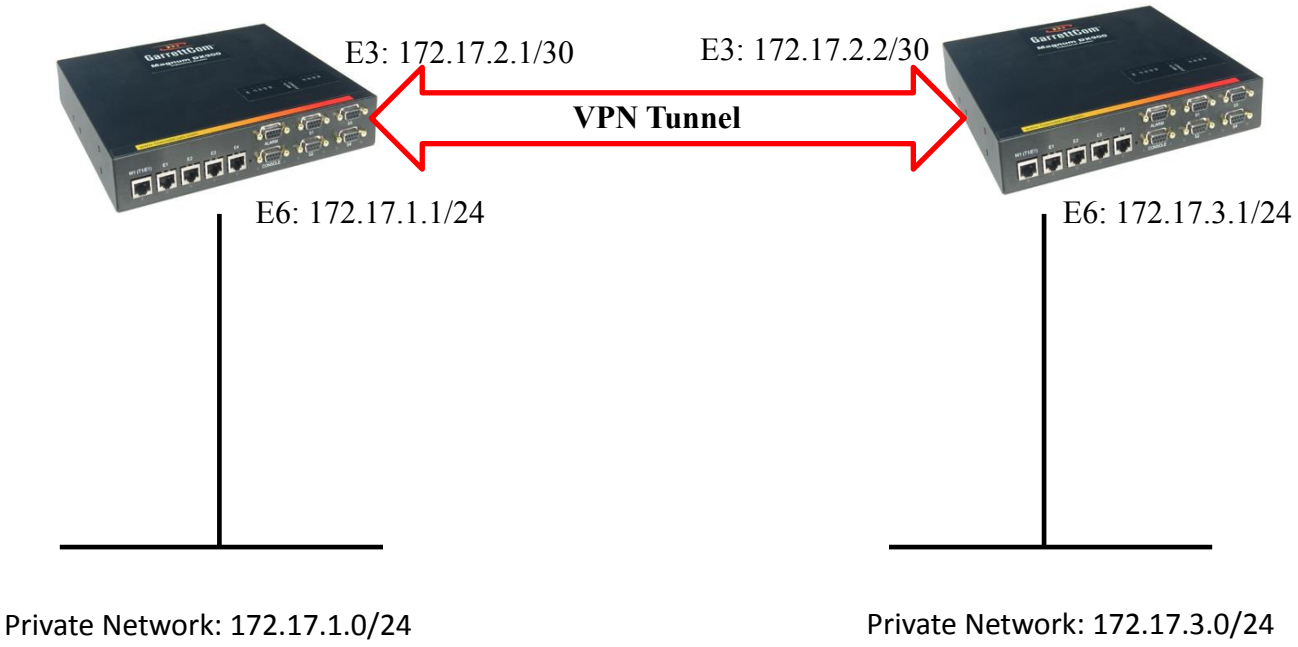
lumbergautomation A BELDEN BRAND
HIRSCHMANN A BELDEN BRAND
TOFINO SECURITY A BELDEN BRAND
GarrettCom A BELDEN BRAND

Belden, Belden Sending All The Right Signals, Hirschmann, GarrettCom, Tofino Security, Lumberg Automation and the Belden logo are trademarks or registered trademarks of Belden Inc. or its affiliated companies in the United States and other jurisdictions. Belden and other parties may also have trademark rights in other terms used herein.

Overview

The Magnum DX Series devices support VPN Tunneling. The following steps will take you through all steps of a basic example on how to configure a functional VPN tunnel.

In the below example, all the traffic traversing between networks 172.17.1.x to network 172.17.3.x and vice versa has to be encrypted and routed through the VPN tunnel between the routers of the two sites.

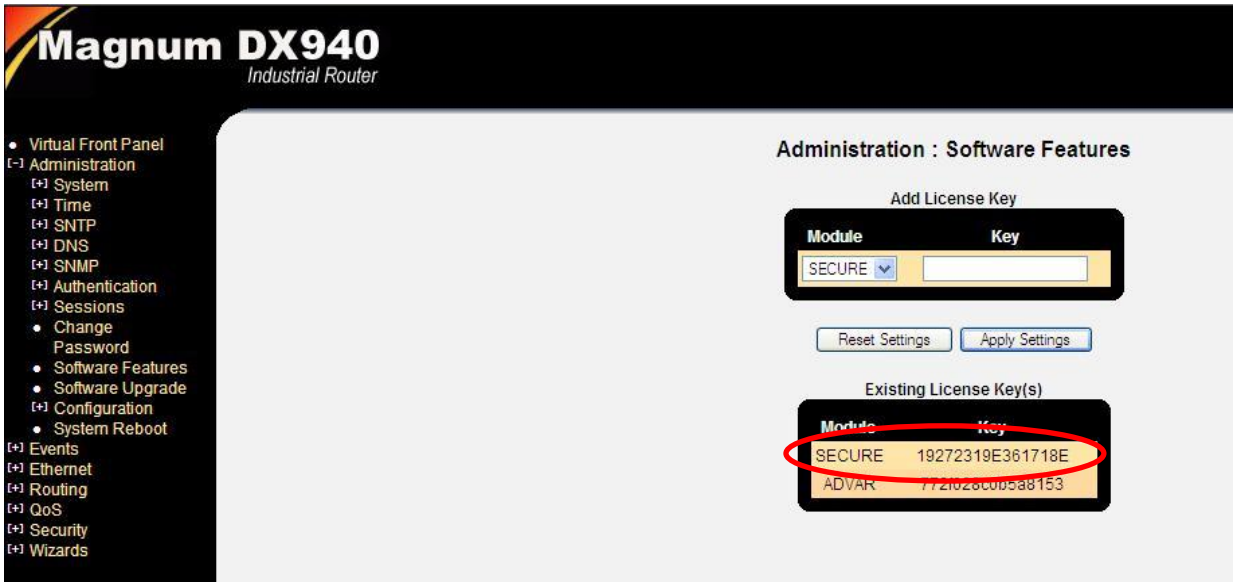


Belden, Belden Sending All The Right Signals, Hirschmann, GarrettCom, Tofino Security, Lumberg Automation and the Belden logo are trademarks or registered trademarks of Belden Inc. or its affiliated companies in the United States and other jurisdictions. Belden and other parties may also have trademark rights in other terms used herein.

Configuration Steps:

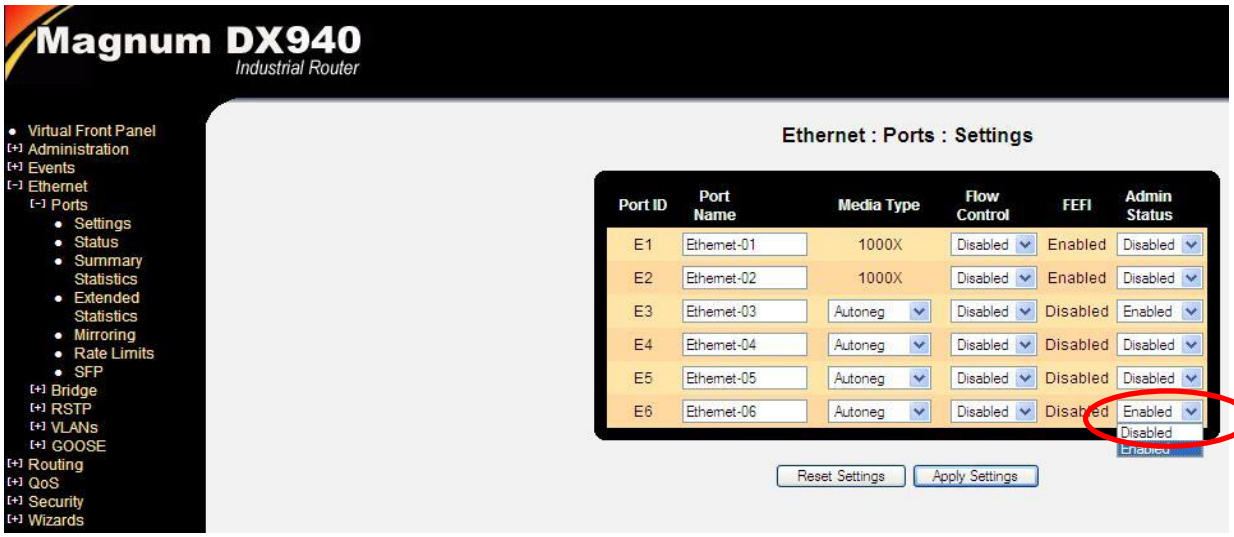
1. Log into DX Router

2. To enable VPN, the router needs have the MNS-DX-SECURE license. Go to Administration> Software Features and make sure that you have MNS-DX-SECURE license installed. If you do not have secure license, then please call 1-855-400-9071 and choose Option 2 to get a quotation.



Belden, Belden Sending All The Right Signals, Hirschmann, GarrettCom, Tofino Security, Lumberg Automation and the Belden logo are trademarks or registered trademarks of Belden Inc. or its affiliated companies in the United States and other jurisdictions. Belden and other parties may also have trademark rights in other terms used herein.

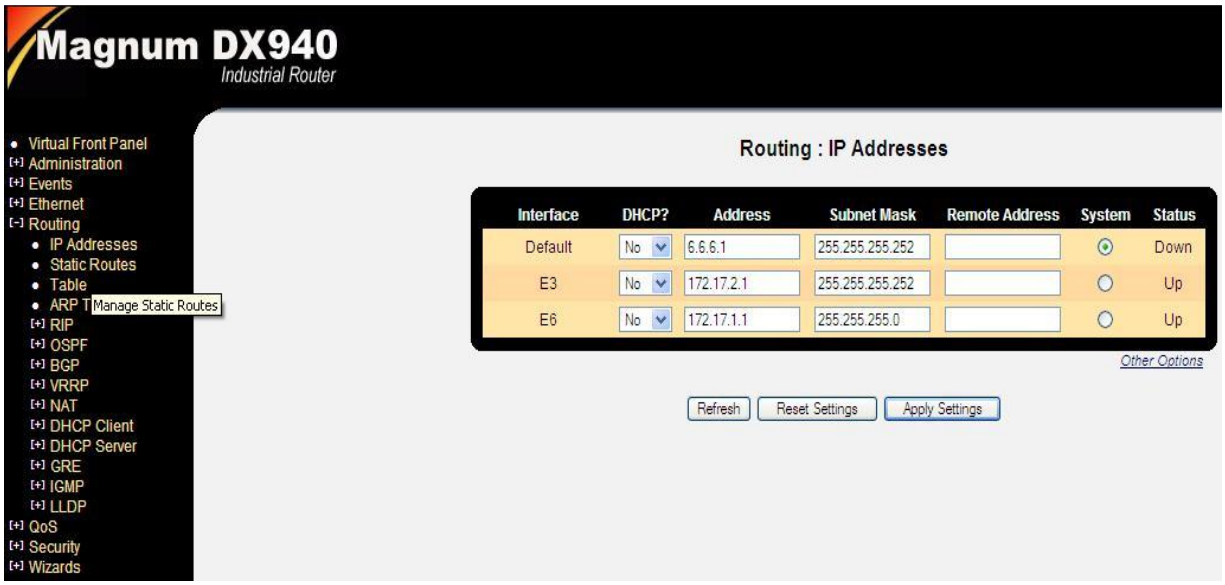
3. Check that ports have been administratively enabled. Go to Ethernet > Ports > Settings. If they are not, then we have to enable the ports by selecting "enabled" from the Admin Status of the respective port(s).



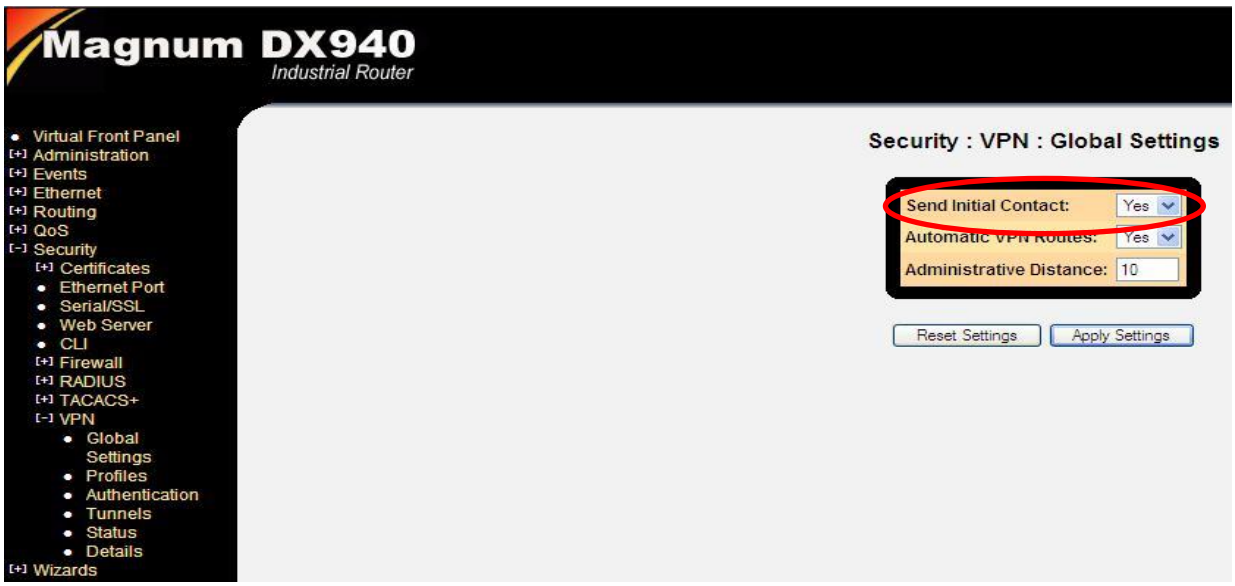
4. By default, the Ethernet ports on the DX routers are configured as switch ports. This step involves "unbridging" the switchports and making them router ports. To unbridge a port, go to Ethernet > Bridge > Settings and choose "No" under "Bridged?" option for the respective port(s).

Belden, Belden Sending All The Right Signals, Hirschmann, GarrettCom, Tofino Security, Lumberg Automation and the Belden logo are trademarks or registered trademarks of Belden Inc. or its affiliated companies in the United States and other jurisdictions. Belden and other parties may also have trademark rights in other terms used herein.

5. Check and assign the IP address and subnet mask (if not already assigned) to the router interfaces. Go to Routing > IP Addresses.



6. This part configures the VPN. Go to Security > VPN > Global Settings. Here the users have to determine if the local router will initiate a VPN connection to the remote site when it sees interesting traffic. If it will, then “Send Initial Contact” should be set to “Yes”. If the local router will only respond to the VPN request from remote router then “Send Initial Contact” should be set to “No”. In our test case, we will set both local and remote routers to initiate the contact to setup the tunnel.



Belden, Belden Sending All The Right Signals, Hirschmann, GarrettCom, Tofino Security, Lumberg Automation and the Belden logo are trademarks or registered trademarks of Belden Inc. or its affiliated companies in the United States and other jurisdictions. Belden and other parties may also have trademark rights in other terms used herein.

7. This step involves creating a profile that will determine the encryption algorithm and hash parameters for the Internet Key Exchange (IKE) and the frames (ESP) of the interesting traffic that will traverse between the router peers. Go to Security > VPN > Profiles.

8. The VPN peers use authentication to form a trust relationship. The trust relationship could be established by either a pre-shared key, which can be a string of combination of alphanumeric and special characters. The same key has to be entered in both the peers. We could also use certificates that two peers might use to authenticate themselves to each other. Go to Security > VPN > Authentication to specify a shared key or certificate.

Belden, Belden Sending All The Right Signals, Hirschmann, GarrettCom, Tofino Security, Lumberg Automation and the Belden logo are trademarks or registered trademarks of Belden Inc. or its affiliated companies in the United States and other jurisdictions. Belden and other parties may also have trademark rights in other terms used herein.

9. Here we define which source and destination traffic will be encrypted and sent via the VPN tunnel. Go to Security > VPN > Tunnel.

This completes the VPN configuration. Now we can start some traffic between the networks 172.17.1.x and 172.17.3.x and see VPN status and details. Please turn over to the next page.

Belden, Belden Sending All The Right Signals, Hirschmann, GarrettCom, Tofino Security, Lumberg Automation and the Belden logo are trademarks or registered trademarks of Belden Inc. or its affiliated companies in the United States and other jurisdictions. Belden and other parties may also have trademark rights in other terms used herein.

10. Check the status of VPN tunnel. If the configurations on both the VPN peers is good, the VPN tunnel will come "Up". Go to Security > VPN > Status.

11. Finally check the traffic statistics through the VPN tunnel. Go to Security > VPN > Details.

Belden, Belden Sending All The Right Signals, Hirschmann, GarrettCom, Tofino Security, Lumberg Automation and the Belden logo are trademarks or registered trademarks of Belden Inc. or its affiliated companies in the United States and other jurisdictions. Belden and other parties may also have trademark rights in other terms used herein.