

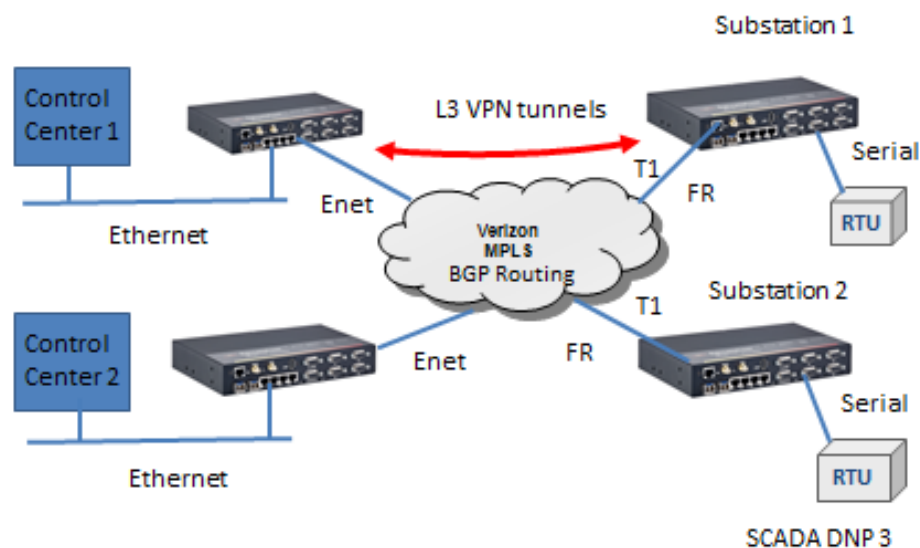
DX940e - Router configuration for a SCADA application over Verizon MPLS

John M - 2019-12-23 - DX/10XTS Routers

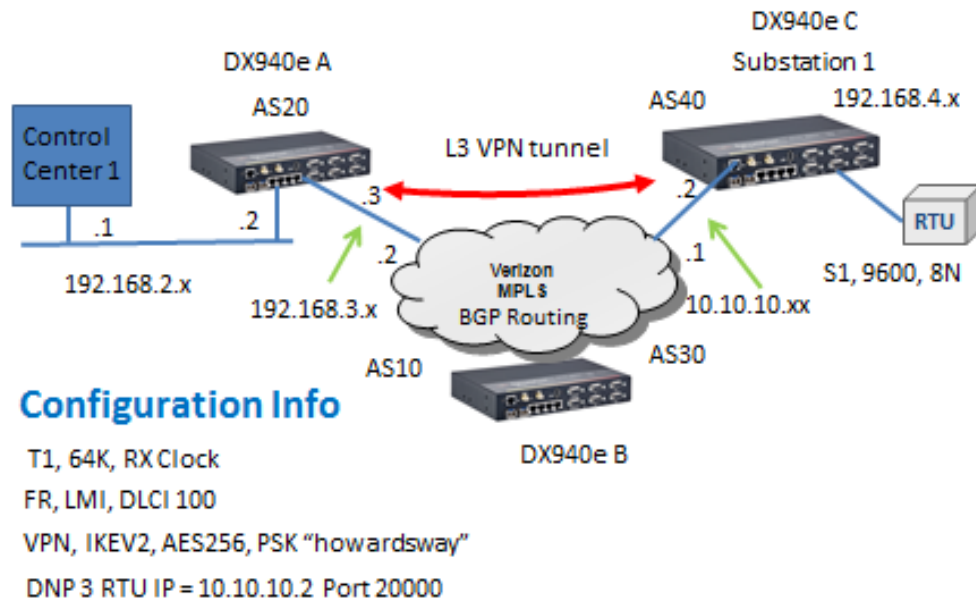
Overview

This example steps through the various configuration screens to setup a SCADA application using a DX940e's at both the headend and remote sites using Verizon MPLS service offering.

For redundancy, each Control center has simultaneous connections to each remote serial attached RTU and employs L3 VPN tunnels for security.



Configuration Information used in this example:



Accessing the DX940e Configuration system

The initial access to DX940e configuration system can be accessed by direct connection to the units console connection, or via an IP based connection using Telnet or SSH. Access to the WEB interface can be achieved using a WEB browser. If this is a new unit the factory default IP address is 192.168.1.2. Please also note that all ports on a factory default setting will be disabled with the exception of the **highest** Ethernet port number. So for a DX940e connect your PC initially to E6.

If you can't access the DX940e via the Ethernet port, because its address is unknown, then the IP address can be reset via the Console port BOOT application. Using a PC Terminal application such as Putty or TeraTerm and connect to the dedicated CONSOLE port (38,400 bps, no parity, 8 data bits and 1 stop bit) using a standard DB9 cross over cable (supplied with the equipment) and holding down the SPACE bar after a DX940e power cycle.

GarrettCom, Inc.

MNS-DX ROM version 3.1.7 (Y12) 200/128

***** Hold down SPACE to stop boot process *****

Starting boot menu...

Boot Menu

1: View System Information

2: Assign System IP Address

3: Install Initial Software Image from FTP Server

4: Install Initial Software Image via TFTP

5: Install Initial Software Image via XMODEM

6: Load Temporary Image from FTP Server

7: Load Temporary Image via TFTP

8: Load Temporary Image via XMODEM

9: Restore System to Factory Defaults

b: Boot

MNS-DX>

Simply use Option 2: to define the initial IP address, then Option b: to boot.

You could also use option "9" to reset all configurations to factory default and the initial IP address of the DX940e would be 192.168.1.2.

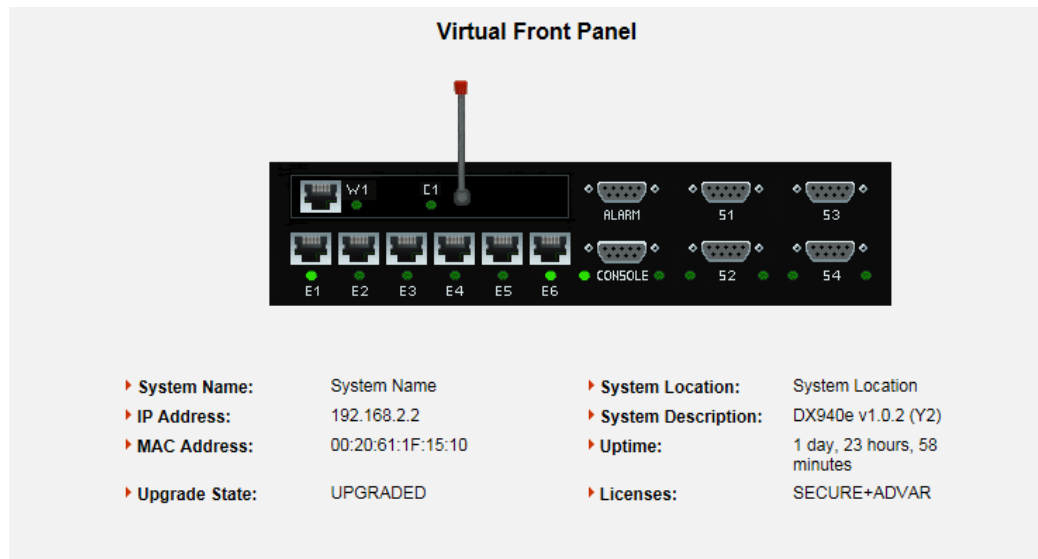
Once IP addresses have been assigned one can access to the configuration system, this section covers WEB access.

Once the address is defined then launch a HTTPS: session to the address that was defined. For this example we are using 192.168.2.2
Mask 255.255.255.0.

Please note that only SECURE access methods are enabled by default, so we need to use HTTPS for WEB access, SSH or Direct console for CLI access.



Default passwords for ADMIN access is “manager/manager”



Initial Virtual Front Panel Web screen showing various system level information including software version etc.

Configurations for DX940e A (Control Center)

Overview of configurations steps

1. Naming the Dx940e
2. Ethernet ports
3. Un bridging an Ethernet Port
4. IP address assignments
5. BGP routing
6. VPN setup
7. Saving configurations

Naming the DX940e

- Virtual Front Panel
- [-] Administration
 - [-] System
 - Information
 - Status
 - Netstat

The Administration menu gives a few options for naming/location and contact..

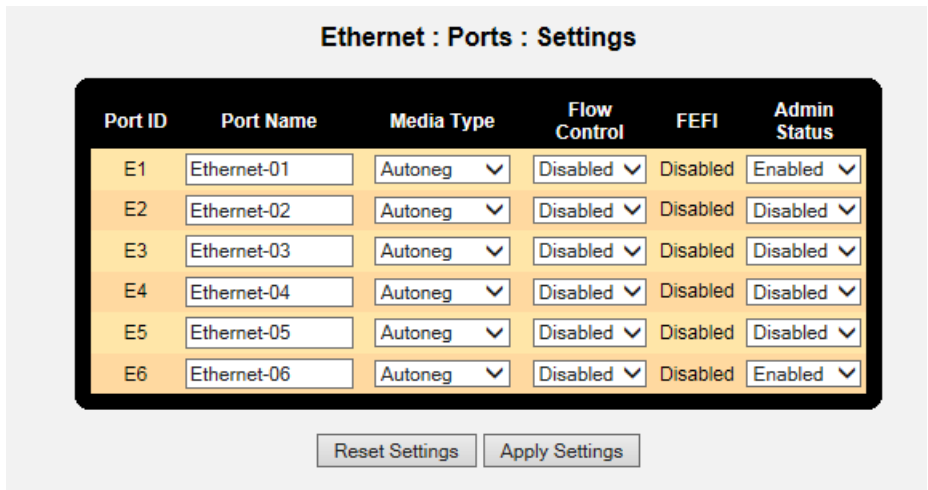
Administration : System : Information

| | |
|---------------------|--------------------|
| System Name: | DX940e A |
| System Location: | Control Center |
| System Contact: | System Contact |
| System Mode: | Normal ▾ |
| System Prompt: | MagnumDX |
| TCP KeepAlive: | 15 |
| System Description: | DX940e v1.0.2 (Y2) |
| Serial Number: | 680100036 |
| Licenses: | SECURE+ADVAR |
| Upgrade State: | UPGRADED |
| IP Address: | 192.168.2.2 |
| MAC Address: | 00:20:61:1F:15:10 |
| Free Space (KB): | 51206 |
| Uptime: | 3 days, 6 minutes |

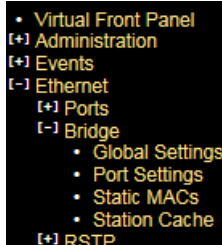
Ethernet Interface Settings

- Virtual Front Panel
- [+] Administration
- [+] Events
- [-] Ethernet
 - [+] Ports
 - [+] Bridge
 - [+] RSTP
 - [+] VLANs
 - [+] GOOSE
- [+] Serial
- [+] WAN
- [+] Cellular
- [+] PPP
- [+] Routing
- [+] QoS
- [+] Security
- [+] Wizards

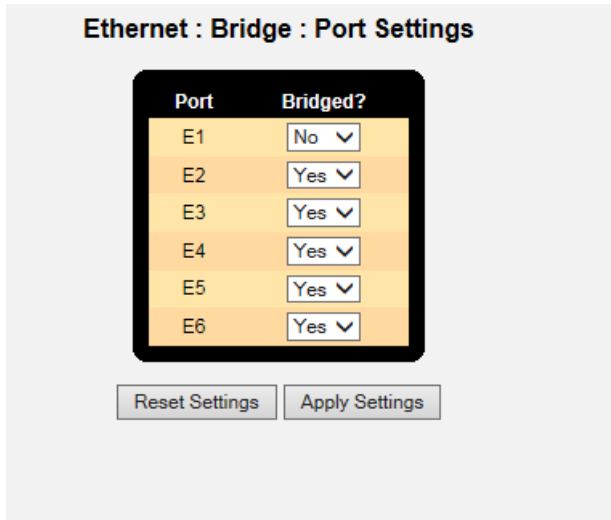
By default all Ethernet ports are ADMIN DISBALED except for port 6. So we need to enable the ports we want to use, in this case E1.



Also by default all Ethernet ports are bridged and only holds one IP address. In this case we are routing between the Control center and Verizon MPLS network with 2 different subnets, so we need un-bridge at least one port to form 2 subnets.

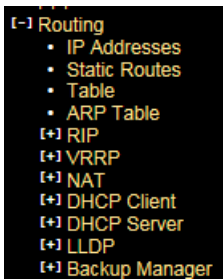


So here we have un-bridged E1 forming a second sub-net



IP addresses

We had previously set the IP address of the DX940e to 192.168.2.2/24 but it can be changed from within this sub-menu.



So with an Ethernet port unbridged we now have two IP subnets, so fill in E1 to 192.168.3.3

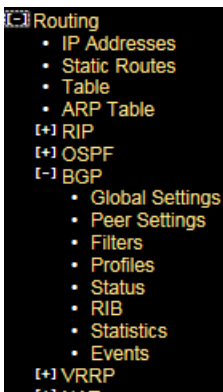
Routing : IP Addresses

| Interface | DHCP? | Address | Subnet Mask | Remote Address | System | Status |
|-----------|-------|-------------|---------------|----------------|----------------------------------|--------|
| Default | No | 192.168.2.2 | 255.255.255.0 | | <input checked="" type="radio"/> | Up |
| E1 | No | 192.168.3.3 | 255.255.255.0 | | <input type="radio"/> | Up |
| CELL1 | No | | | | <input type="radio"/> | Down |

[Other Options](#)

BGP Routing

When using a Verizon carrier service like MPLS this usually requires BGP as the routing protocol of preference.



Starting with Global Settings we enable to feature, assign the AS number, and the Router ID which is simply the IP address of the Ethernet port connecting to the Verizon MPLS service.

Routing : BGP : Global Settings

| | |
|----------------------|-------------|
| BGP Mode: | Enabled |
| AS Number: | 20 |
| Router ID: | 192.168.3.3 |
| eBGP Admin Distance: | 20 |
| iBGP Admin Distance: | 200 |
| Include Ext OSPF: | Disabled |
| Event Level: | High |

Next BGP Peer Settings, IP addresses for each end of the connection and associated AS numbers. Here I left the Profile as “default” but we will make changes to that profile next.

Routing : BGP : Peer Settings

Add Peer

| BGP Name | Peer IP Address | Local IP Address | Peer AS | Local AS | Hold Timer (sec) | Profile | Input Filter | Output Filter | MD5 Password |
|----------|-----------------|------------------|---------|----------|------------------|---------|--------------|---------------|--------------|
| bgp-1 | 0.0.0.0 | 0.0.0.0 | 1 | 1 | 40 | Default | NONE | NONE | |

Existing Peers

| BGP Name | Peer IP Address | Local IP Address | Peer AS | Local AS | Hold Timer (sec) | Profile | Input Filter | Output Filter | MD5 Password | Delete |
|----------|-----------------|------------------|---------|----------|------------------|---------|--------------|---------------|--------------|--------------------------|
| bgp-1 | 192.168.3.2 | 192.168.3.3 | 10 | 20 | 40 | Default | NONE | NONE | | <input type="checkbox"/> |

Modify the “default” profile next, here we have selected “Redist Static and BGP”, this just means we will share information of local IP addresses into the BGP protocol and also learnt IP addresses through BGP placed into the routing table.

Routing : BGP : Profiles

Add New Profile

| Profile Name | Default Router | Redist Static | Redist RIP | Redist OSPF | Redist BGP | Weight | Private AS | Local Pref | TCP Passive |
|--------------|----------------|---------------|------------|-------------|------------|--------|------------|------------|-------------|
| New Profile | No | No | No | No | No | 100 | No | 100 | No |

Existing Profiles

| Profile Name | Default Router | Redist Static | Redist RIP | Redist OSPF | Redist BGP | Weight | Private AS | Local Pref | TCP Passive | Delete |
|--------------|----------------|---------------|------------|-------------|------------|--------|------------|------------|-------------|--------------------------|
| Default | No | Yes | No | No | Yes | 100 | Yes | 100 | No | <input type="checkbox"/> |

If the unit is connected to the Verizon circuit we should see status information similar to this

Routing : BGP : Status

| Neighbor | Version | AS # | BGP State | Nets Rcvd | Pkts Sent | Pkts Rcvd | TCP/MD5 Session | Reset |
|-------------|---------|------|-------------|-----------|-----------|-----------|-----------------|-------|
| 192.168.3.2 | 4 | 10 | Established | 2 | 16982 | 17339 | No | None |

And the RIB table populated with learnt IP addresses.

Routing : BGP : RIB

| Prefix | Bits | Source Peer # | Source AS# | Number Hops | Weight | Origin | Local Pref | eBGP/iBGP |
|-------------|------|---------------|------------|-------------|--------|--------|------------|-----------|
| 10.10.10.0 | 24 | 192.168.3.2 | 10 | 1 | 100 | 2 | 0 | e |
| 192.168.4.0 | 24 | 192.168.3.2 | 40 | 2 | 100 | 1 | 0 | e |

Finally a look at the full IP routing table to check we have full connectivity of the network

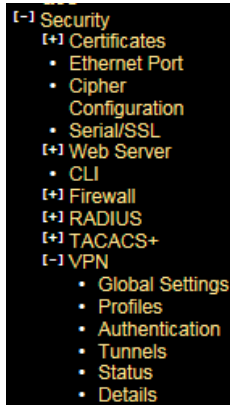
Routing : Table

| Route Destination | Route Mask | Next Hop | Administrative Distance | Metric | Age | Type |
|-------------------|-----------------|-------------|-------------------------|--------|--------|-------|
| 10.10.10.0 | 255.255.255.0 | 192.168.3.2 | 1 | 0 | | VPN |
| 127.0.0.1 | 255.255.255.255 | 127.0.0.1 | 0 | 0 | | |
| 192.168.2.0 | 255.255.255.0 | 192.168.2.2 | 0 | 0 | | Local |
| 192.168.2.2 | 255.255.255.255 | 192.168.2.2 | 0 | 0 | | |
| 192.168.3.0 | 255.255.255.0 | 192.168.3.3 | 0 | 0 | | Local |
| 192.168.3.3 | 255.255.255.255 | 192.168.3.3 | 0 | 0 | | |
| 192.168.4.0 | 255.255.255.0 | 192.168.3.2 | 20 | 0 | 177072 | BGP |

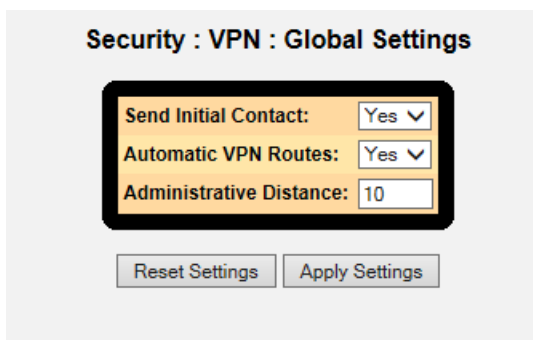
VPN Setup

Since we are using a Public Verizon MPLS service where it might be possible that the SCADA information could be eavesdropped we use a VPN tunnel to provide both authentication and encryption services for the

SCADA traffic.

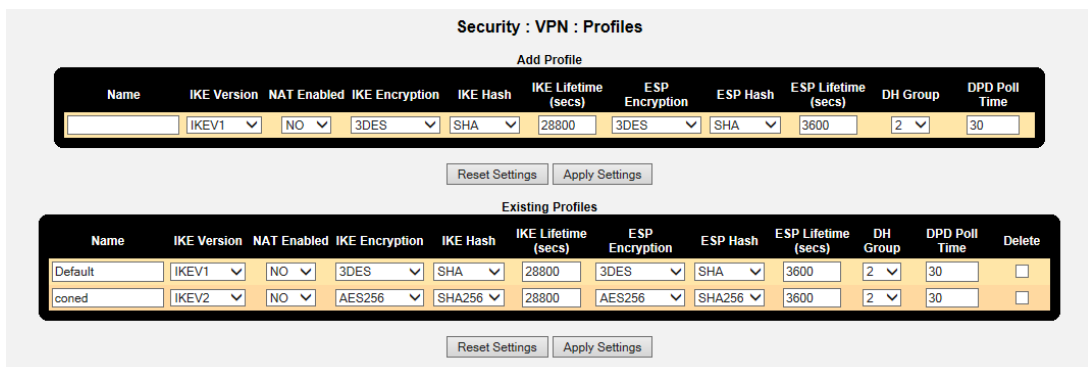


Starting with Global Settings, turn on “send initial contact”



Next we build a new profile and selected the version of the IPsec VPN and the encryption settings for the Authentication and Data Transfer phases.

Here I selected the most secure settings, IPsec version IKEV2, AES256 encryption strength and both IKE and ESP Hash to SHA256.



Now for the actual authentication “shared secret”, we can use Pre-Shared Key or you may prefer to build your own private certificates, not covered

here. The Pre-shared Key method is just a string of characters, like a password, that is used during authentication of the 2 VPN peers. In this example it was set to "howardsway". As you can see the string is not displayed for security purposes but it is set.

Security : VPN : Authentication

Add Method

| Name | Type | Preshared Key | Preshared Key Verify | Local Certificate |
|----------------------|------|----------------------|----------------------|-------------------|
| <input type="text"/> | PSK | <input type="text"/> | <input type="text"/> | None |

Existing Methods

| Name | Type | Preshared Key | Preshared Key Verify | Local Certificate | Delete |
|---------|------|----------------------|----------------------|-------------------|--------------------------|
| Default | PSK | <input type="text"/> | <input type="text"/> | None | <input type="checkbox"/> |
| coned | PSK | <input type="text"/> | <input type="text"/> | None | <input type="checkbox"/> |

With all that set we can finally define the tunnel end points , so we want the tunnel to exist throughout the Verizon network, so in this example we want any traffic between 192.168.2.x and 10.10.10.x , ie the Control Station network and remote RTU network and be protected throughout the "public" network and using the new profile and authentication methods. Note the Destination gateway is the IP address of the substation DX940e WAN port and we also selected that the VPN be up and available at all times.

Security : VPN : Tunnels

Add Tunnel

| Source Address | Source Mask | Destination Address | Destination Mask | Destination Gateway | Profile | Authentication | Protocol | Always Up |
|----------------------|----------------------|----------------------|----------------------|----------------------|---------|----------------|----------|-----------|
| <input type="text"/> | <input type="text"/> | <input type="text"/> | <input type="text"/> | <input type="text"/> | Default | Default | any | No |

Existing VPN Tunnels

| ID | Source Address | Source Mask | Destination Address | Destination Mask | Destination Gateway | Profile | Authentication | Protocol | Always Up | Delete |
|----|----------------|---------------|---------------------|------------------|---------------------|---------|----------------|----------|-----------|--------------------------|
| 1 | 192.168.2.0 | 255.255.255.0 | 10.10.10.0 | 255.255.255.0 | 10.10.10.2 | coned | coned | any | Yes | <input type="checkbox"/> |

Successful VPN connection can be verified

Security : VPN : Status

Tunnel Statistics

| ID | Source Address | Destination Address | Next Hop | Status | Time Remaining (secs) | Restart |
|----|----------------|---------------------|------------|--------|-----------------------|--------------------------|
| 1 | 192.168.2.0 | 10.10.10.0 | 10.10.10.2 | VPN up | 2555 | <input type="checkbox"/> |

Security : VPN : Details

| Source Address | Destination Address | Inbound SPI | Outbound SPI | Remaining Time (secs) | Inbound Packets | Outbound Packets |
|----------------|---------------------|-------------|--------------|-----------------------|-----------------|------------------|
| 192.168.2.0 | 10.10.10.0 | FD4FB110 | 84276FB2 | 2530 | 4 | 4 |

Saving Configurations

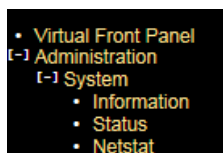
Please make sure you SAVE the configurations we have made by hitting the "SAVE" ICON at the bottom right of the WEB screen, the button is highlighted when there are configurations that have not been saved.

Configurations for DX940e C (Substation Locations)

Overview of configurations steps

1. Naming the Dx940e
2. Ethernet ports
3. T1 WAN Port
4. Frame Relay
5. IP address assignments
6. BGP routing
7. VPN setup
8. Serial Ports
9. Terminal Server
10. Saving configurations

Naming the DX940e



The Administration menu gives a few options for naming/location and contact..

A screenshot of the 'Administration : System : Information' configuration page. The page has a light gray background and a central white box with a black border containing the configuration fields. At the bottom of the page are three buttons: 'Refresh', 'Reset Settings', and 'Apply Settings'.

| Administration : System : Information | |
|---------------------------------------|---|
| System Name: | <input type="text" value="DX940e C"/> |
| System Location: | <input type="text" value="Substation Locations"/> |
| System Contact: | <input type="text" value="System Contact"/> |
| System Mode: | <input type="text" value="Normal"/> ▼ |
| System Prompt: | <input type="text" value="MagnumDX"/> |
| TCP KeepAlive: | <input type="text" value="15"/> |
| System Description: | DX940e v1.0.2 (Y2) |
| Serial Number: | 680100046 |
| Licenses: | SECURE+ADVAR |
| Upgrade State: | UPGRADED |
| IP Address: | 192.168.4.2 |
| MAC Address: | 00:20:61:1F:0F:90 |
| Free Space (KB): | 51431 |
| Uptime: | 2 days, 23 hours, 59 minutes |

Ethernet Ports

There is no requirement for ethernet ports for this application.

T1 WAN Port

- WAN
 - Settings
 - Status
 - Statistics
 - Frame Relay
 - FR Statistics
 - DLCI Settings
 - DLCI Status
 - Switch Settings
 - EEK Settings
 - EEK Status

Physical port settings for the T1 interface, set timeslot bandwidth to 64k, Clock Received and Admin enable, all other values leave as defaults

WAN : Port Settings

| Port ID | Port Name | Timeslot Bandwidth | Clock | Admin Status | Mode | Time Slots | Frame Types | Line Codes | Line Build Out |
|---------|-----------|--------------------|----------|--------------|------|------------|-------------|------------|----------------|
| W1 | WAN-01 | 64k | Received | Enabled | T1 | 1-24 | ESF (T1) | B8ZS (T1) | 0to133 |

If this is correct then looking at T1 status should look like this.

WAN : Port Status

| Port ID | Line State | LMI State | Oper State |
|---------|------------|-----------|------------|
| W1 | OK | Up | Up |

Then we select if we want to employ the LMI management channel, unfortunately there are 3 variants, but Verizon uses CISCO and so the LMI type should be the original LMI version, and select User role.

WAN : Frame Relay

| Port ID | Fragmentation Size | LMI Type | LMI Mode | TxQ Mode | Token Q Pct |
|---------|--------------------|----------|----------|----------|-------------|
| W1 | 0 | LMI | User | 8421 | 70 |

Last step here is to define a DLCI for the IP traffic application, here with picked DLCI 100, but the actual DLCI would have been provided by Verizon. Set the application for this DLCI to IP=YES and Layer3-IP.

WAN : DLCI Settings

Add DLCI

| Port ID | DLCI | CIR | IP | EEK | TYPE |
|---------|------|-----|-----|------|-----------|
| W1 | | | Yes | None | Layer3-IP |

Existing DLCIs

| Port ID | DLCI | CIR | IP | EEK | TYPE | Delete |
|---------|------|-----|-----|------|-----------|--------------------------|
| W1 | 100 | | Yes | None | Layer3-IP | <input type="checkbox"/> |

[Vendor Specific Details](#)

The status the DLCI can be seen here.

WAN : DLCI Status

| Port ID | DLCI | State | Rx Packets | Rx Octets | Tx Packets | Tx Octets | Rx Drops | Tx Drops |
|---------|------|--------|------------|-----------|------------|-----------|----------|----------|
| W1 | 100 | Active | 64005 | 4461561 | 72364 | 5527556 | 0 | 0 |

IP addresses

We had previously set the IP address of the DX940e to 192.168.2.4/24 but it can be changed from within this sub-menu. We only will use port 6 for web interface configuration.



So with simply add in a new IP address for the WAN port 10.10.10.2/24

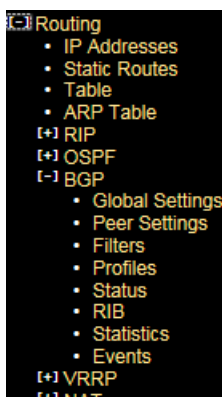
Routing : IP Addresses

| Interface | DHCP? | Address | Subnet Mask | Remote Address | System | Status |
|-------------|-------|-------------|---------------|----------------|----------------------------------|--------|
| Default | No | 192.168.4.2 | 255.255.255.0 | | <input checked="" type="radio"/> | Up |
| W1-DLCI 100 | No | 10.10.10.2 | 255.255.255.0 | | <input type="radio"/> | Up |
| CELL1 | No | | | | <input type="radio"/> | Down |

[Other Options](#)

BGP Routing

When using a Verizon carrier service like MPLS this usually requires BGP as the routing protocol of preference.



Starting with Global Settings we enable to feature, assign the AS number, and the Router ID which is simply the IP address of the Ethernet port connecting to the Verizon MPLS service.

Routing : BGP : Global Settings

| | |
|----------------------|------------|
| BGP Mode: | Enabled |
| AS Number: | 40 |
| Router ID: | 10.10.10.2 |
| eBGP Admin Distance: | 20 |
| iBGP Admin Distance: | 200 |
| Include Ext OSPF: | Disabled |
| Event Level | High |

Next BGP Peer Settings, IP addresses for each end of the connection and associated AS numbers. Here I left the Profile as “default” but we will make changes to that profile next.

Routing : BGP : Peer Settings

Add Peer

| BGP Name | Peer IP Address | Local IP Address | Peer AS | Local AS | Hold Timer (sec) | Profile | Input Filter | Output Filter | MD5 Password |
|----------|-----------------|------------------|---------|----------|------------------|---------|--------------|---------------|--------------|
| bgp-1 | 0.0.0.0 | 0.0.0.0 | 1 | 1 | 40 | Default | NONE | NONE | |

Existing Peers

| BGP Name | Peer IP Address | Local IP Address | Peer AS | Local AS | Hold Timer (sec) | Profile | Input Filter | Output Filter | MD5 Password | Delete |
|----------|-----------------|------------------|---------|----------|------------------|---------|--------------|---------------|--------------|--------------------------|
| FR-link | 10.10.10.1 | 10.10.10.2 | 30 | 40 | 40 | Default | NONE | NONE | | <input type="checkbox"/> |

Modify the "default" profile next, here we have selected "Redist Static and BGP", this just means we will share information of local IP addresses into the BGP protocol and also learnt IP addresses through BGP placed into the routing table.

Routing : BGP : Profiles

Add New Profile

| Profile Name | Default Router | Redist Static | Redist RIP | Redist OSPF | Redist BGP | Weight | Private AS | Local Pref | TCP Passive |
|--------------|----------------|---------------|------------|-------------|------------|--------|------------|------------|-------------|
| New Profile | No | No | No | No | No | 100 | No | 100 | No |

Existing Profiles

| Profile Name | Default Router | Redist Static | Redist RIP | Redist OSPF | Redist BGP | Weight | Private AS | Local Pref | TCP Passive | Delete |
|--------------|----------------|---------------|------------|-------------|------------|--------|------------|------------|-------------|--------------------------|
| Default | No | Yes | No | No | Yes | 100 | Yes | 100 | No | <input type="checkbox"/> |

If the unit is connected to the Verizon circuit we should see status information similar to this

Routing : BGP : Status

| Neighbor | Version | AS # | BGP State | Nets Rcvd | Pkts Sent | Pkts Rcvd | TCP/MD5 Session | Reset |
|------------|---------|------|-------------|-----------|-----------|-----------|-----------------|-------|
| 10.10.10.1 | 4 | 30 | Established | 2 | 125 | 127 | No | None |

And the RIB table populated with learnt IP addresses.

Routing : BGP : RIB

| Prefix | Bits | Source Peer # | Source AS# | Number Hops | Weight | Origin | Local Pref | eBGP/iBGP |
|-------------|------|---------------|------------|-------------|--------|--------|------------|-----------|
| 192.168.3.0 | 24 | 10.10.10.1 | 30 | 1 | 100 | 2 | 0 | e |
| 192.168.2.0 | 24 | 10.10.10.1 | 20 | 2 | 100 | 1 | 0 | e |

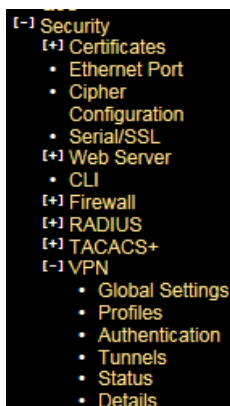
Finally a look at the full IP routing table to check we have full connectivity of the network

Routing : Table

| Route Destination | Route Mask | Next Hop | Administrative Distance | Metric | Age | Type |
|-------------------|-----------------|-------------|-------------------------|--------|------|-------|
| 10.10.10.0 | 255.255.255.0 | 10.10.10.2 | 0 | 0 | | Local |
| 10.10.10.2 | 255.255.255.255 | 10.10.10.2 | 0 | 0 | | |
| 127.0.0.1 | 255.255.255.255 | 127.0.0.1 | 0 | 0 | | |
| 192.168.2.0 | 255.255.255.0 | 10.10.10.1 | 1 | 0 | | VPN |
| 192.168.3.0 | 255.255.255.0 | 10.10.10.1 | 20 | 0 | 5658 | BGP |
| 192.168.4.0 | 255.255.255.0 | 192.168.4.2 | 0 | 0 | | Local |
| 192.168.4.2 | 255.255.255.255 | 192.168.4.2 | 0 | 0 | | |

VPN Setup

Since we are using a Public Verizon MPLS service where it might be possible that the SCADA information could be eavesdropped we use a VPN tunnel to provide both authentication and encryption services for the SCADA traffic.



Starting with Global Settings, turn on "send initial contact"

Security : VPN : Global Settings

Send Initial Contact:

Automatic VPN Routes:

Administrative Distance:

Next we build a new profile and selected the version of the IPsec VPN and the encryption settings for the Authentication and Data Transfer phases.

Here I selected the most secure settings, IPsec version IKEV2, AES256 encryption strength and both IKE and ESP Hash to SHA256.

Security : VPN : Profiles

Add Profile

| Name | IKE Version | NAT Enabled | IKE Encryption | IKE Hash | IKE Lifetime (secs) | ESP Encryption | ESP Hash | ESP Lifetime (secs) | DH Group | DPD Poll Time |
|----------------------|------------------------------------|---------------------------------|-----------------------------------|----------------------------------|------------------------------------|-----------------------------------|----------------------------------|-----------------------------------|--------------------------------|---------------------------------|
| <input type="text"/> | <input type="text" value="IKEV1"/> | <input type="text" value="NO"/> | <input type="text" value="3DES"/> | <input type="text" value="SHA"/> | <input type="text" value="28800"/> | <input type="text" value="3DES"/> | <input type="text" value="SHA"/> | <input type="text" value="3600"/> | <input type="text" value="2"/> | <input type="text" value="30"/> |

Existing Profiles

| Name | IKE Version | NAT Enabled | IKE Encryption | IKE Hash | IKE Lifetime (secs) | ESP Encryption | ESP Hash | ESP Lifetime (secs) | DH Group | DPD Poll Time | Delete |
|---------|------------------------------------|---------------------------------|-------------------------------------|-------------------------------------|------------------------------------|-------------------------------------|-------------------------------------|-----------------------------------|--------------------------------|---------------------------------|--------------------------|
| Default | <input type="text" value="IKEV1"/> | <input type="text" value="NO"/> | <input type="text" value="3DES"/> | <input type="text" value="SHA"/> | <input type="text" value="28800"/> | <input type="text" value="3DES"/> | <input type="text" value="SHA"/> | <input type="text" value="3600"/> | <input type="text" value="2"/> | <input type="text" value="30"/> | <input type="checkbox"/> |
| coned | <input type="text" value="IKEV2"/> | <input type="text" value="NO"/> | <input type="text" value="AES256"/> | <input type="text" value="SHA256"/> | <input type="text" value="28800"/> | <input type="text" value="AES256"/> | <input type="text" value="SHA256"/> | <input type="text" value="3600"/> | <input type="text" value="2"/> | <input type="text" value="30"/> | <input type="checkbox"/> |

Now for the actual authentication “shared secret”, we can use Pre-Shared Key or you may prefer to build your own private certificates, not covered here. The Pre-shared Key method is just a string of characters, like a password, that is used during authentication of the 2 VPN peers. In this example it was set to “howardsway”. As you can see the string is not displayed for security purposes but it is set.

Security : VPN : Authentication

Add Method

| Name | Type | Preshared Key | Preshared Key Verify | Local Certificate |
|----------------------|----------------------------------|----------------------|----------------------|-----------------------------------|
| <input type="text"/> | <input type="text" value="PSK"/> | <input type="text"/> | <input type="text"/> | <input type="text" value="None"/> |

Existing Methods

| Name | Type | Preshared Key | Preshared Key Verify | Local Certificate | Delete |
|---------|----------------------------------|----------------------|----------------------|-----------------------------------|--------------------------|
| Default | <input type="text" value="PSK"/> | <input type="text"/> | <input type="text"/> | <input type="text" value="None"/> | <input type="checkbox"/> |
| coned | <input type="text" value="PSK"/> | <input type="text"/> | <input type="text"/> | <input type="text" value="None"/> | <input type="checkbox"/> |

With all that set we can finally define the tunnel end points, so we want the tunnel to exist throughout the Verizon network, so in this example we want any traffic between 192.168.2.x and 10.10.10.x , ie the Control Station network and remote RTU network and be protected throughout the “public” network and using the new profile and authentication methods. Note the Destination gateway is the IP address of the substation DX940e WAN port and we also selected that the VPN be up and available at all times.

Security : VPN : Tunnels

Add Tunnel

| Source Address | Source Mask | Destination Address | Destination Mask | Destination Gateway | Profile | Authentication | Protocol | Always Up |
|----------------------|----------------------|----------------------|----------------------|----------------------|---------|----------------|----------|-----------|
| <input type="text"/> | <input type="text"/> | <input type="text"/> | <input type="text"/> | <input type="text"/> | Default | Default | any | No |

Existing VPN Tunnels

| ID | Source Address | Source Mask | Destination Address | Destination Mask | Destination Gateway | Profile | Authentication | Protocol | Always Up | Delete |
|----|----------------|---------------|---------------------|------------------|---------------------|---------|----------------|----------|-----------|--------------------------|
| 1 | 10.10.10.0 | 255.255.255.0 | 192.168.2.0 | 255.255.255.0 | 192.168.3.3 | coned | coned | any | No | <input type="checkbox"/> |

Successful VPN connection can be verified

Security : VPN : Status

Tunnel Statistics

| ID | Source Address | Destination Address | Next Hop | Status | Time Remaining (secs) | Restart |
|----|----------------|---------------------|-------------|--------|-----------------------|--------------------------|
| 1 | 10.10.10.0 | 192.168.2.0 | 192.168.3.3 | VPN up | 2156 | <input type="checkbox"/> |

Security : VPN : Details

| Source Address | Destination Address | Inbound SPI | Outbound SPI | Remaining Time (secs) | Inbound Packets | Outbound Packets |
|----------------|---------------------|-------------|--------------|-----------------------|-----------------|------------------|
| 10.10.10.0 | 192.168.2.0 | 3C0C6653 | 4C4AC1DF | 2127 | 11 | 13 |

Serial Ports

- Serial
- Ports
 - Profiles
 - Settings
 - Status
 - Statistics

All serial ports in the default configuration are disabled, so we need to enable the port, and perhaps name it.

Serial : Ports : Settings

| Port ID | Port Name | Profile | Admin Status |
|---------|-----------|---------|--------------|
| S1 | RTU | Default | Enabled |
| S2 | Serial-02 | Default | Disabled |
| S3 | Serial-03 | Default | Disabled |
| S4 | Serial-04 | Default | Disabled |

Next we setup a profile that matches the RTU, Baud, Parity, Stops bits etc. We also need to set "Ignore DSS" to YES, and adjust the Pkt time to 20 versus 200.

Serial : Ports : Profiles

Add New Profile

| Profile Name | Interface Standard | Speed | Data Bits | Stop Bits | Parity | Ignore DSS | Flow Control | Pkt Char | Pkt Time (msecs) | Max Pkt Size (bytes) | T/A Time (msecs) |
|--------------|--------------------|-------|-----------|-----------|--------|------------|--------------|----------|------------------|----------------------|------------------|
| New Profile | RS232 | 9600 | 8 | 1 | None | No | None | None | 200 | 1024 | 0 |

Existing Profiles

| Profile Name | Interface Standard | Speed | Data Bits | Stop Bits | Parity | Ignore DSS | Flow Control | Pkt Char | Pkt Time (msecs) | Max Pkt Size (bytes) | T/A Time (msecs) | Delete |
|--------------|--------------------|-------|-----------|-----------|--------|------------|--------------|----------|------------------|----------------------|------------------|--------------------------|
| Default | RS232 | 9600 | 8 | 1 | None | Yes | None | None | 20 | 1024 | 0 | <input type="checkbox"/> |

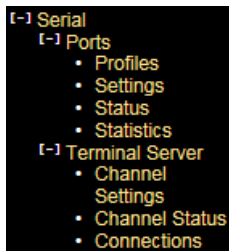
We can check the status, the Ignore DSS parameter enables the port rather than needing additional signals like DTR from the RTU.

Serial : Ports : Status

| Port ID | DCD | CTS | DSR | Oper State |
|---------|-----|-----|-----|------------|
| S1 | Off | Off | Off | Up |
| S2 | Off | Off | Off | Disabled |
| S3 | Off | Off | Off | Disabled |
| S4 | Off | Off | Off | Disabled |

Terminal Server

The terminal server acts as the transition for the IP TCP session carrying DNP3 traffic and passing just the payload to the serial port.



The channel settings shows call direction inbound, allows for any IP to be used, and we simply modified the listening TCP port number to match our DNP3 session, in this case 20000.

Serial : Terminal Server : Channel Settings

Add New Channel

| Port ID | Call Direction | Session Type | Priority (DiffServ) | Payload Offset | Local IP | Local TCP | Remote Name or IP | Remote TCP | Maximum Connections | Retry Time (secs) |
|---------|----------------|--------------|---------------------|----------------|----------|-----------|-------------------|------------|---------------------|-------------------|
| S1 | In | Raw | Default | Yes | Any | 0 | | 0 | 5 | 30 |

Reset Settings Apply Settings

Existing Channels

| Port ID | Call Direction | Session Type | Priority (DiffServ) | Payload Offset | Local IP | Local TCP | Remote Name or IP | Remote TCP | Maximum Connections | Retry Time (secs) | Delete |
|---------|----------------|--------------|---------------------|----------------|----------|-----------|-------------------|------------|---------------------|-------------------|--------------------------|
| S1 | In | Raw | Default | Yes | Any | 20000 | | 0 | 5 | 30 | <input type="checkbox"/> |
| S2 | In | Raw | Default | Yes | Any | 10202 | | 0 | 5 | 30 | <input type="checkbox"/> |
| S3 | In | Raw | Default | Yes | Any | 10203 | | 0 | 5 | 30 | <input type="checkbox"/> |
| S4 | In | Raw | Default | Yes | Any | 10204 | | 0 | 5 | 30 | <input type="checkbox"/> |

Reset Settings Apply Settings

Saving Configurations

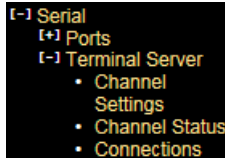
Please make sure you SAVE the configurations we have made by hitting the "SAVE" ICON at the bottom right of the WEB screen, the button is highlighted when there are configurations that have not been saved.



SCADA Host Connection

So to make the SCADA Host connect we simply launch a DNP3 TCP session to the WAN IP port address of the DX940e using the port number "20000". So in this case TCP 10.10.10.2 port 20000.

We can check the connection by looking here at the channel status of the Terminal Server/Serial port



Serial : Terminal Server : Connections

| Port ID | Connection Type | Session Type | Local IP | Local TCP | Remote Name or IP | Remote TCP | Tx Octets | Rx Octets | Delete |
|---------|-----------------|--------------|------------|-----------|-------------------|------------|-----------|-----------|--------------------------|
| S1 | TCP | Raw | 10.10.10.2 | 20000 | 192.168.2.1 | 54882 | 142 | 142 | <input type="checkbox"/> |

Saving Configurations

Please make sure you SAVE the configurations we have made by hitting the "SAVE" ICON at the bottom right of the WEB screen, the button is highlighted when there are configurations that have not been saved.

