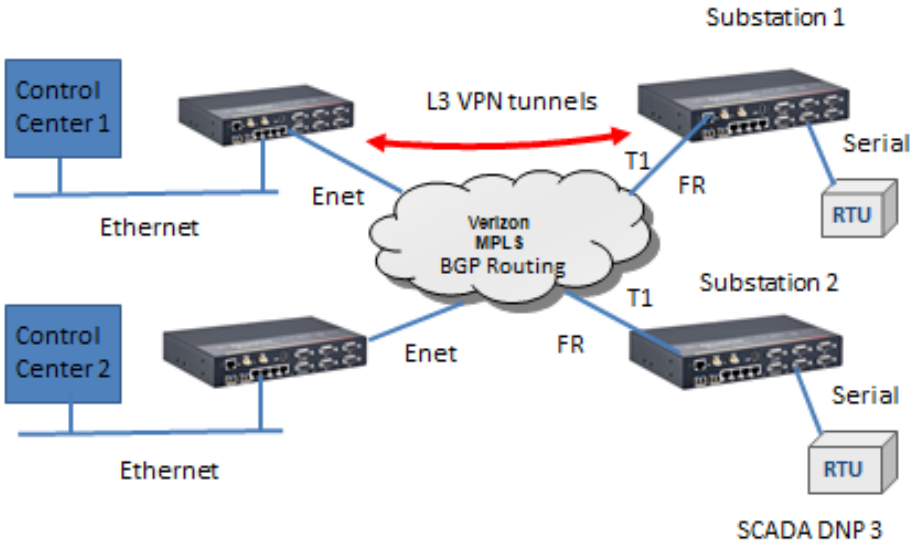
DX940e - Router configuration for a SCADA application over Verizon MPLS

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

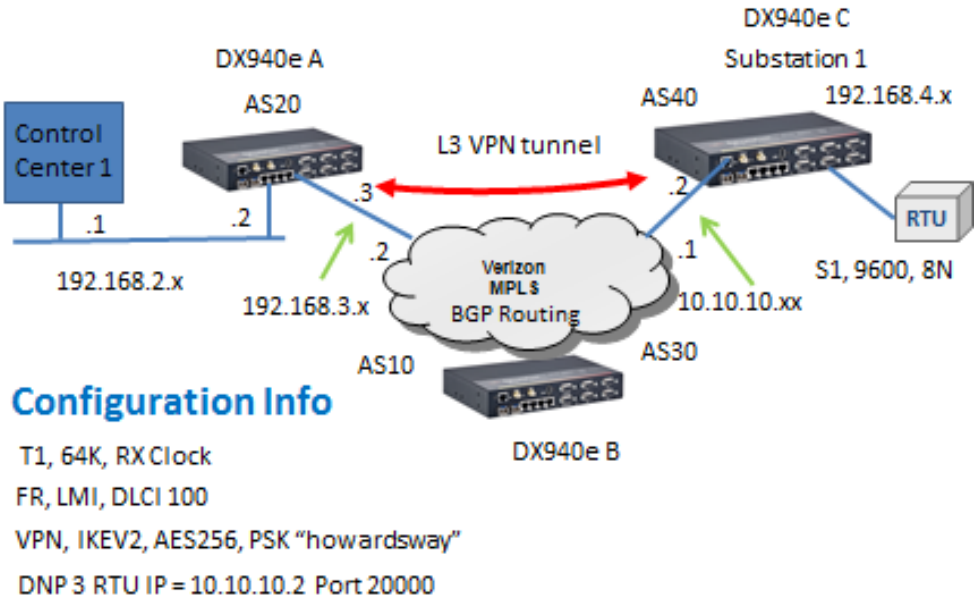
Overview

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

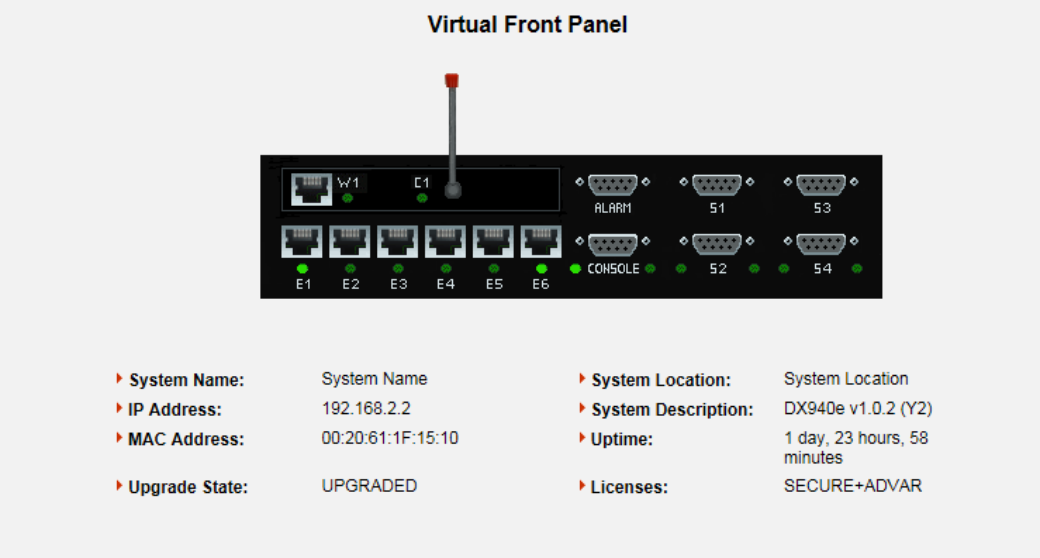
1: View System Information
2: Assign System IP Address
3: Install Initial Software Image from FTP Server
4: Install Initial Software Image via TFTP
5: Install Initial Software Image via XMODEM
6: Load Temporary Image from FTP Server
7: Load Temporary Image via TFTP
8: Load Temporary Image via XMODEM
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”



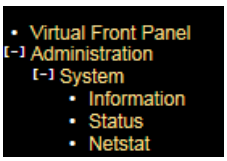
Initial Virtual Front Panel Web screen showing various system level information including software version etc.

Configurations for DX940e A (Control Center)

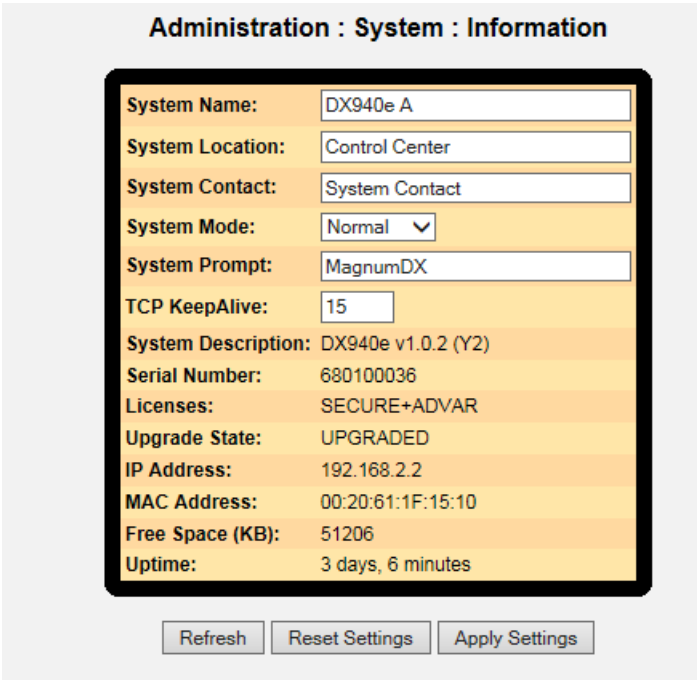
Overview of configurations steps

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

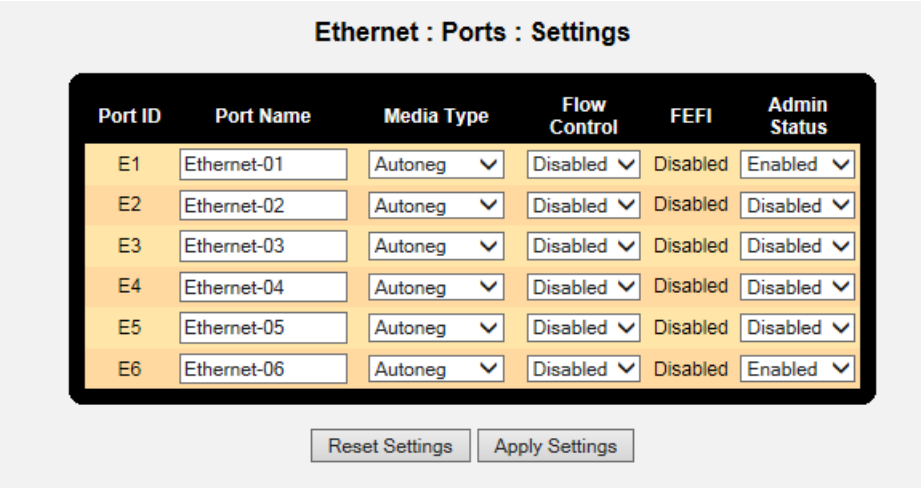


The Administration menu gives a few options for naming/location and contact..

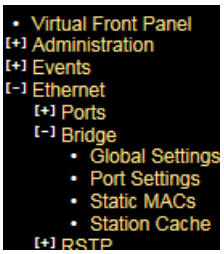


Ethernet Interface Settings

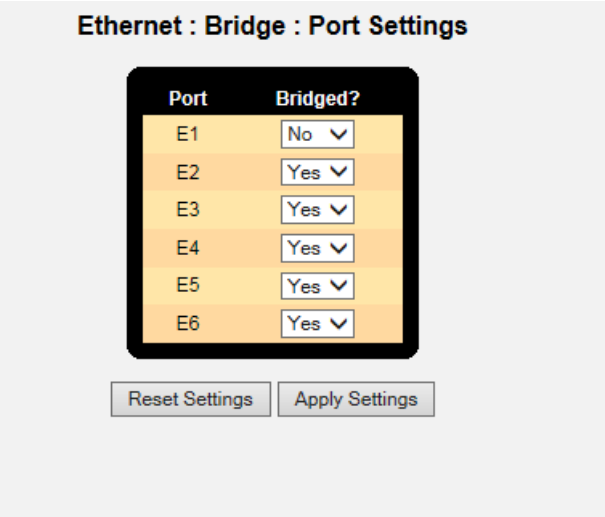
By default all Ethernet ports are ADMIN DISBALED except for port 6. So we need to enable the ports we want to use, in this case E1.



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.

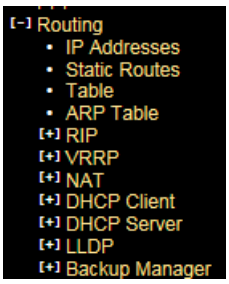


So here we have un-bridged E1 forming a second sub-net

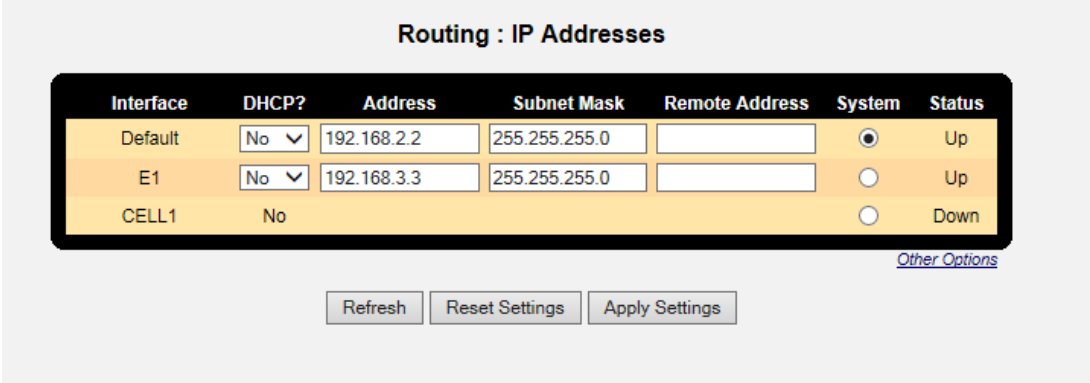


IP addresses

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.

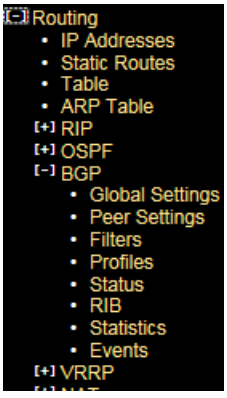


So with an Ethernet port unbridged we now have two IP subnets, so fill in E1 to 192.168.3.3

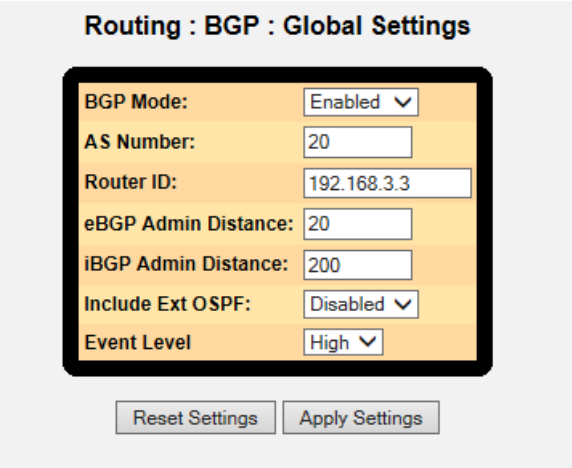


BGP Routing

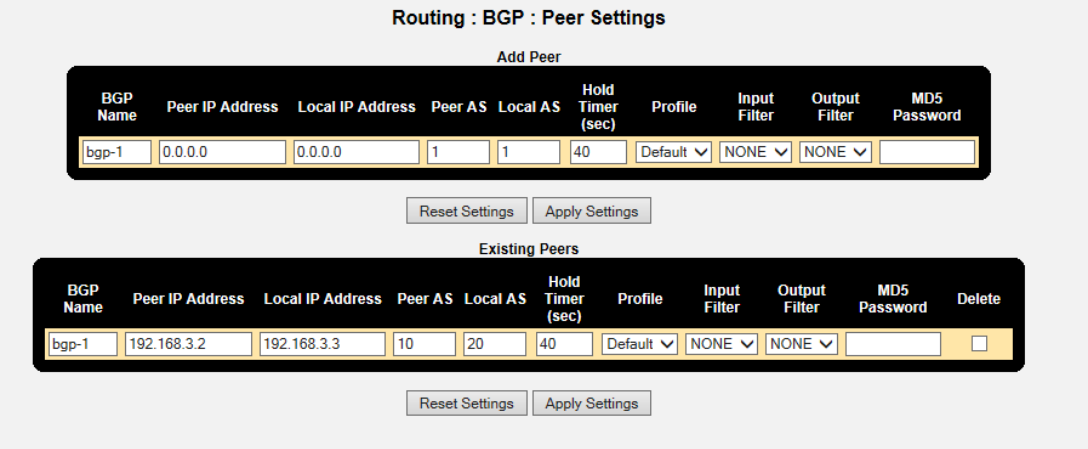
When using a Verizon carrier service like MPLS this usually requires BGP as the routing protocol of preference.



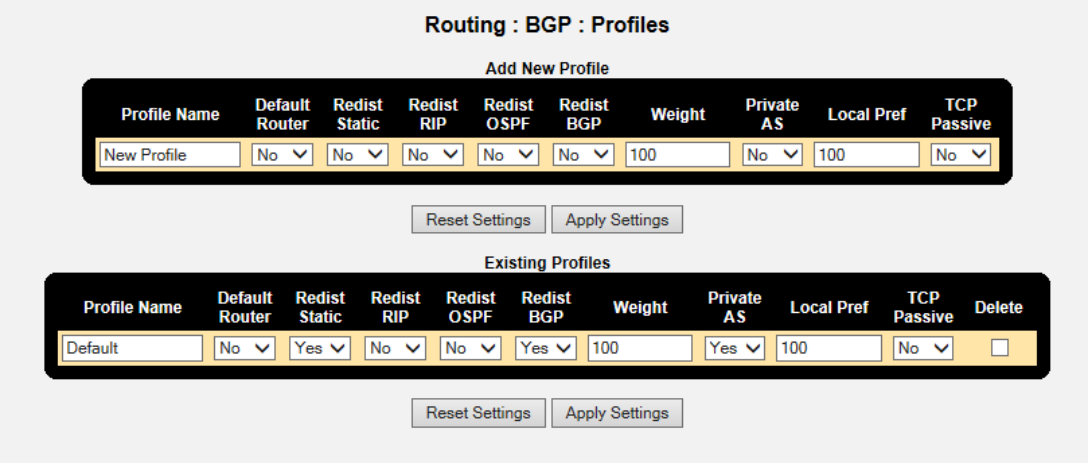
Starting with Global Settings we enable to feature, assign the AS number, and the Router ID which is simply the IP address of the Ethernet port connecting to the Verizon MPLS service.



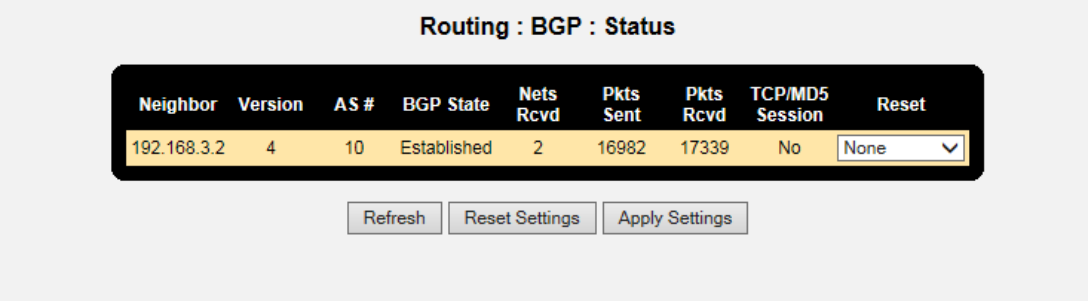
Next BGP Peer Settings, IP addresses for each end of the connection and associated AS numbers. Here I left the Profile as “default” but we will make changes to that profile next.



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.



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

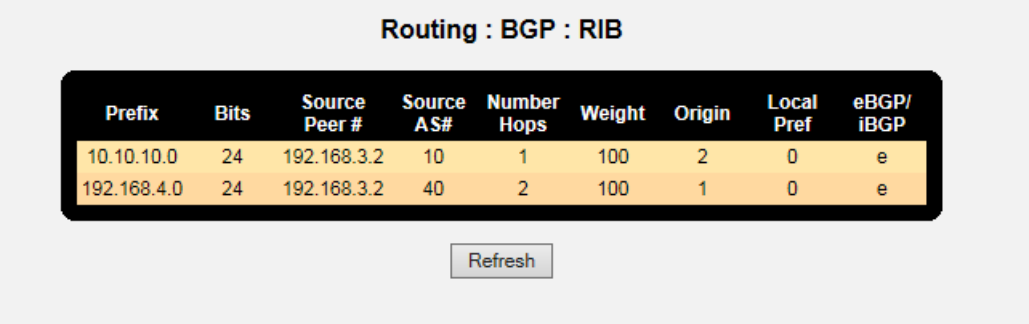


Routing : BGP : Status

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

Refresh | Reset Settings | Apply Settings

And the RIB table populated with learnt IP addresses.

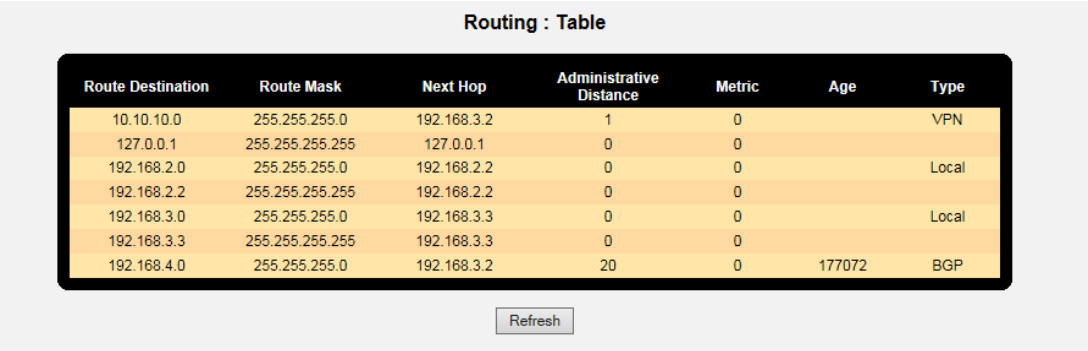


Routing : BGP : RIB

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

Refresh

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



Routing : Table

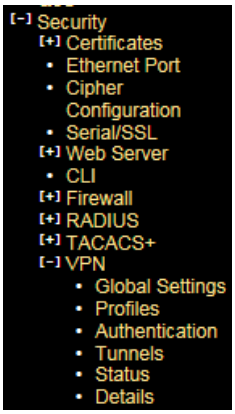
Route Destination	Route Mask	Next Hop	Administrative Distance	Metric	Age	Type
10.10.10.0	255.255.255.0	192.168.3.2	1	0		VPN
127.0.0.1	255.255.255.255	127.0.0.1	0	0		
192.168.2.0	255.255.255.0	192.168.2.2	0	0		Local
192.168.2.2	255.255.255.255	192.168.2.2	0	0		
192.168.3.0	255.255.255.0	192.168.3.3	0	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

Refresh

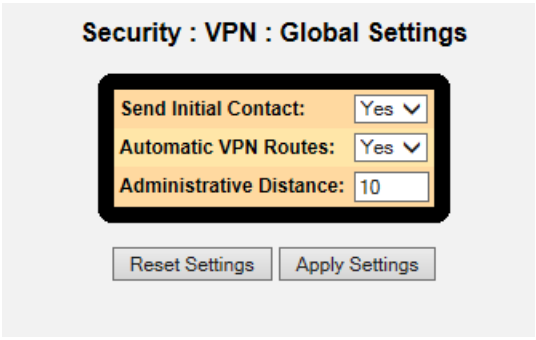
VPN Setup

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.

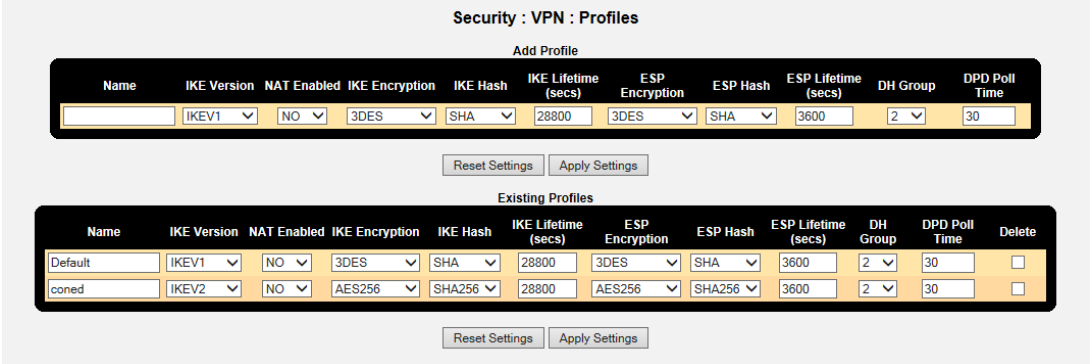


Starting with Global Settings, turn on “send initial contact”



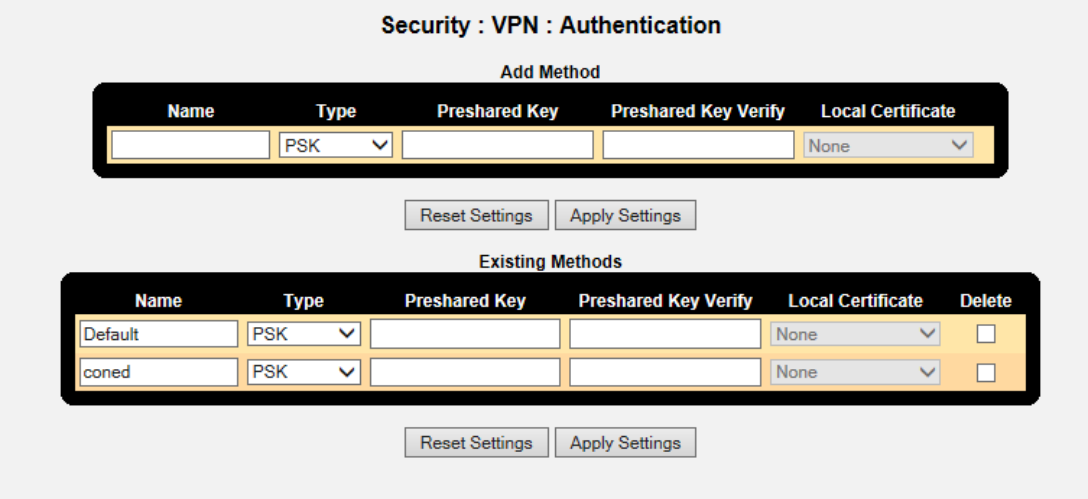
Next we build a new profile and selected the version of the IPSec VPN and the encryption settings for the Authentication and Data Transfer phases.

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

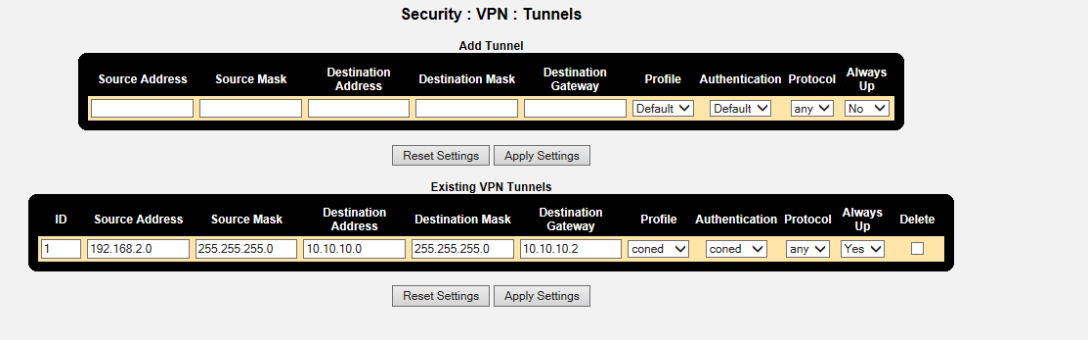


Now for the actual authentication “shared secret”, we can use Pre-Shared Key or you may prefer to build your own private certificates, not covered

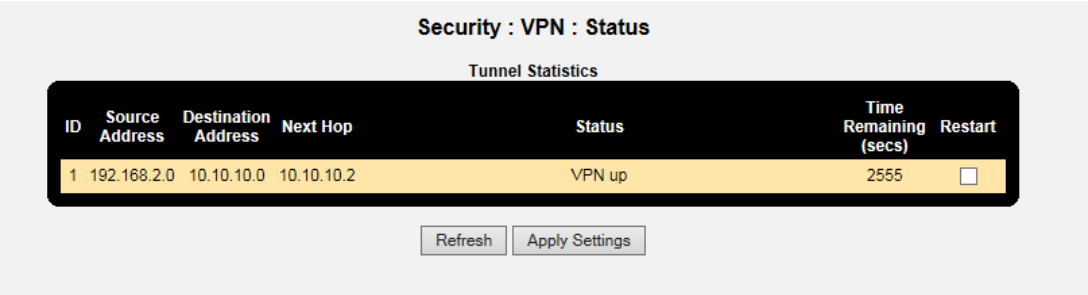
here. The Pre-shared Key method is just a string of characters, like a password, that is used during authentication of the 2 VPN peers. In this example it was set to “howardsway”. As you can see the string is not displayed for security purposes but it is set.

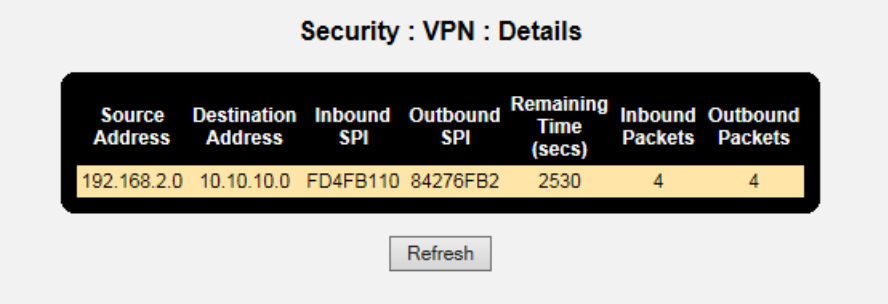


With all that set we can finally define the tunnel end points , so we want the tunnel to exist throughout the Verizon network, so in this example we want any traffic between 192.168.2.x and 10.10.10.x , ie the Control Station network and remote RTU network and be protected throughout the “public” network 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.



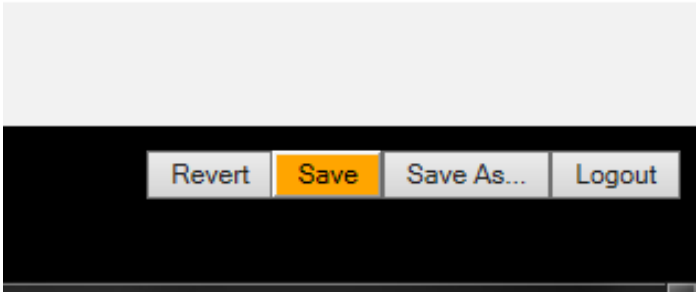
Successful VPN connection can be verified





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.

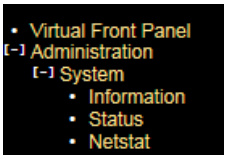


Configurations for DX940e C (Substation Locations)

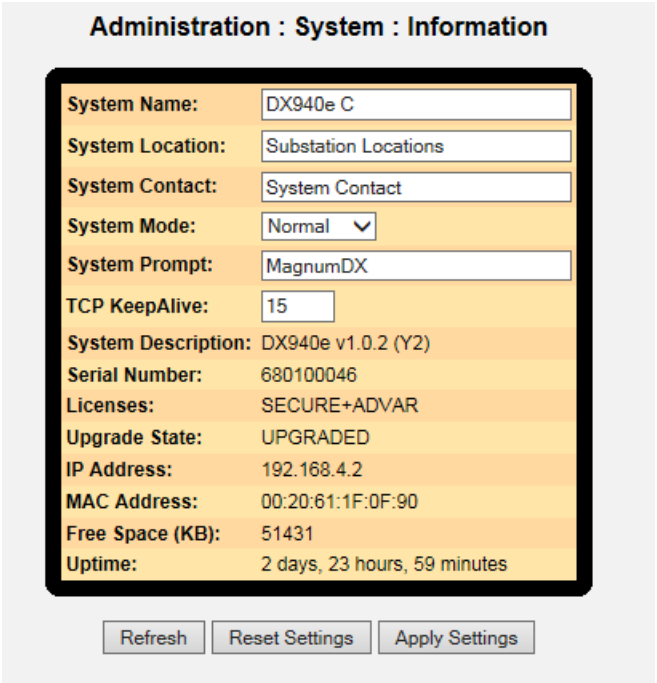
Overview of configurations steps

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



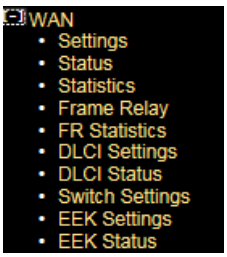
The Administration menu gives a few options for naming/location and contact..



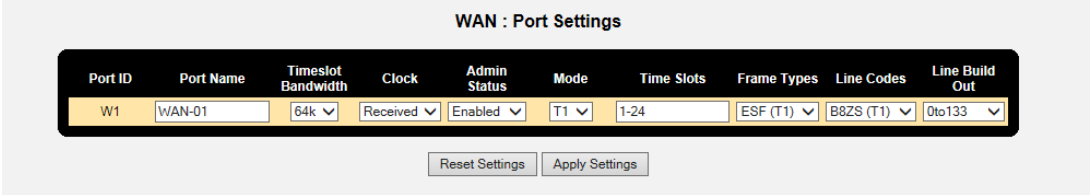
Ethernet Ports

There is no requirment for ethernet ports for this application.

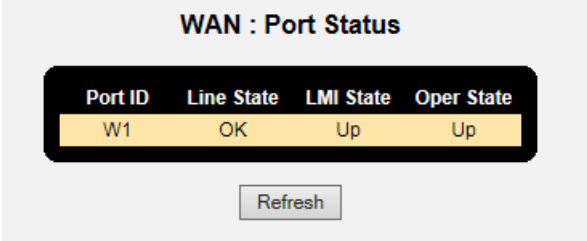
T1 WAN Port



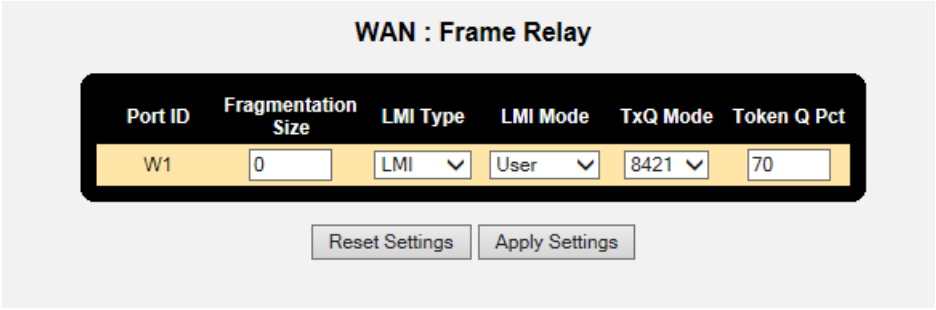
Physical port settings for the T1 interface, set timeslot bandwidth to 64k, Clock Received and Admin enable, all other values leave as defaults



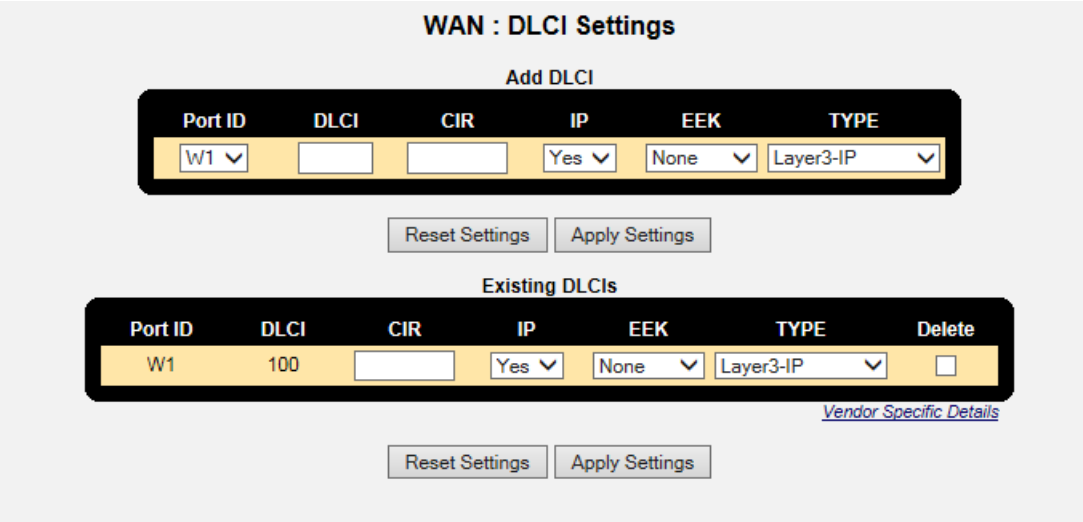
If this is correct then looking at T1 status should look like this.



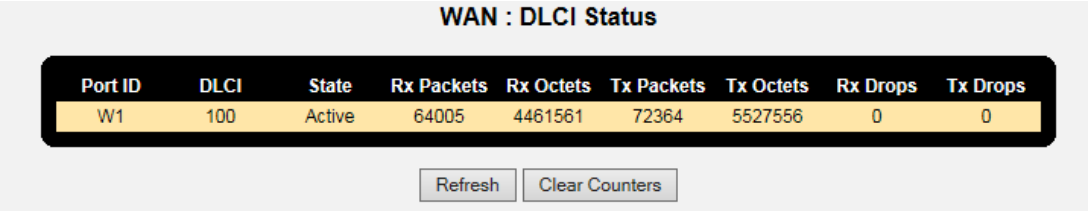
Then we select if we want to employ the LMI management channel, unfortunately there are 3 variants, but Verizon uses CISCO and so the LMI type should be the original LMI version, and select User role.



Last step here is to define a DCLI 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.

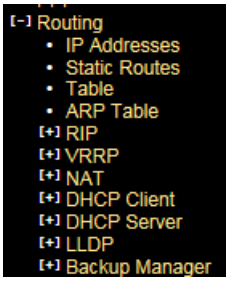


The status the DLCI can be seen here.

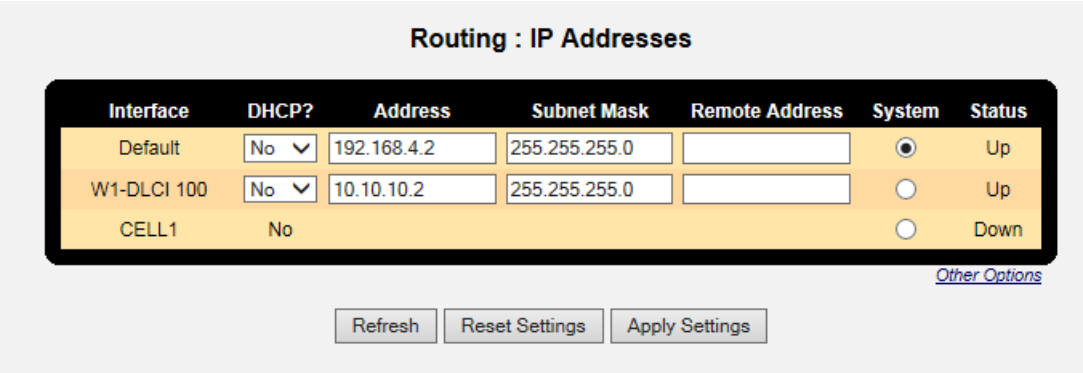


IP addresses

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.

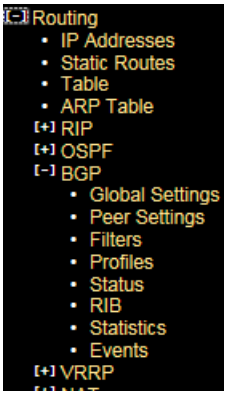


So with simply add in a new IP address for the WAN port 10.10.10.2/24

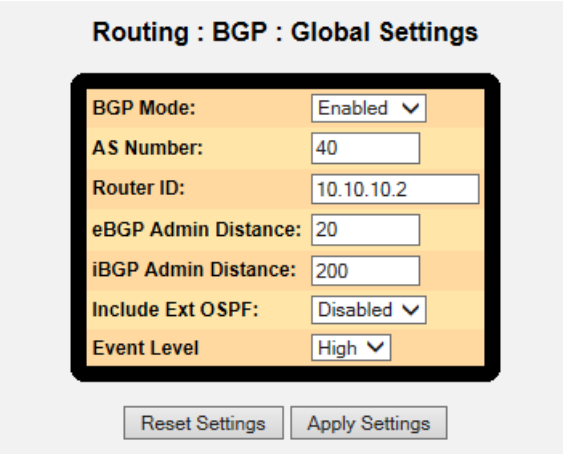


BGP Routing

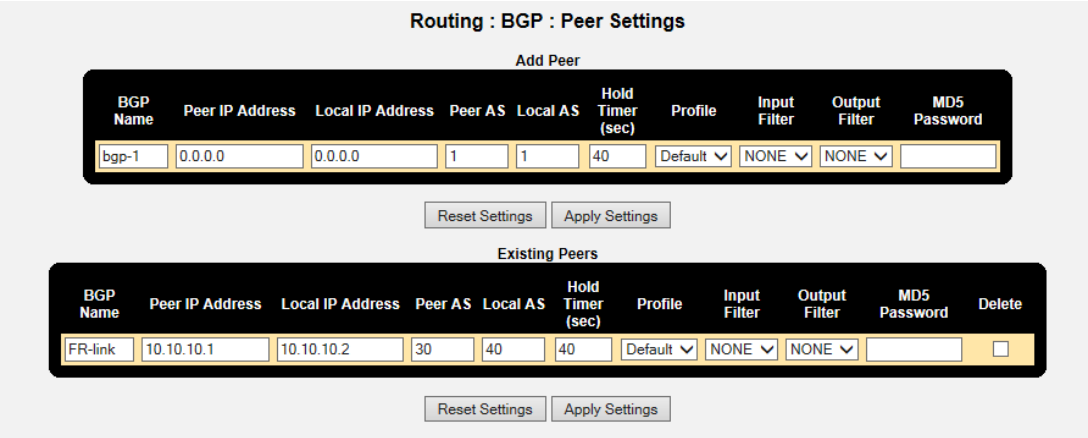
When using a Verizon carrier service like MPLS this usually requires BGP as the routing protocol of preference.



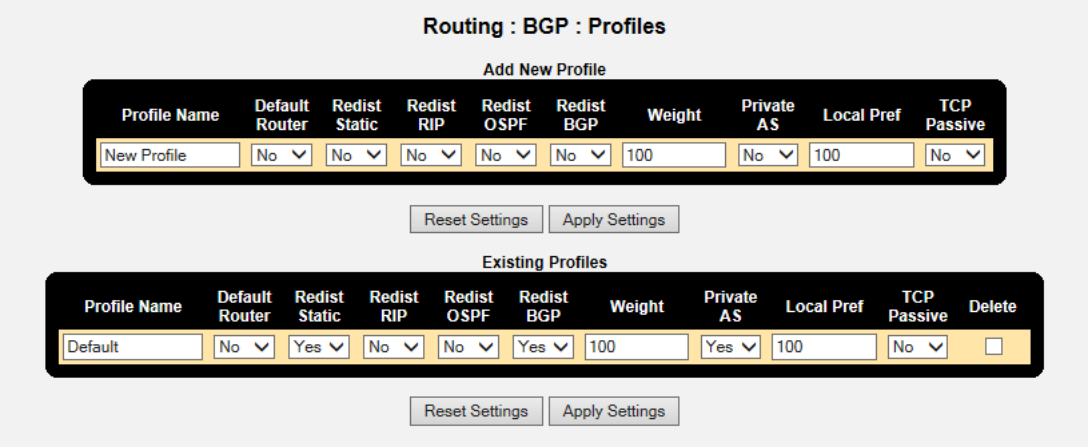
Starting with Global Settings we enable to feature, assign the AS number, and the Router ID which is simply the IP address of the Ethernet port connecting to the Verizon MPLS service.



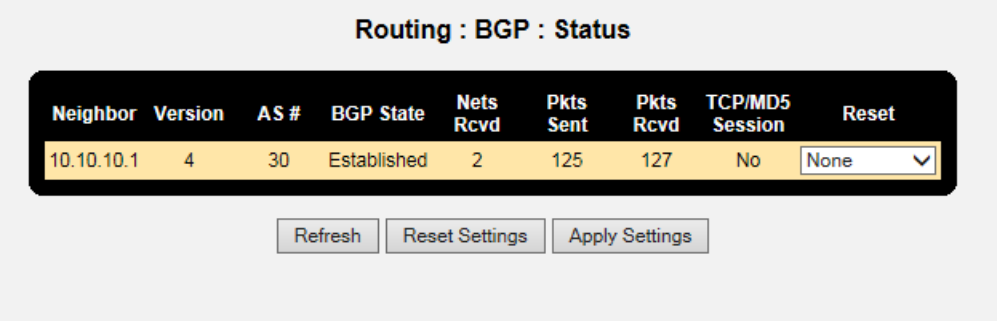
Next BGP Peer Settings, IP addresses for each end of the connection and associated AS numbers. Here I left the Profile as “default” but we will make changes to that profile next.



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.



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



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

Refresh

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

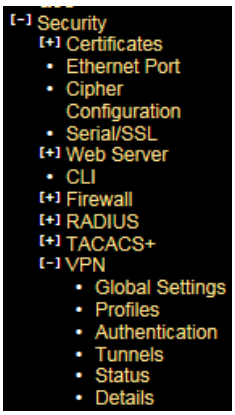
Routing : Table

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		

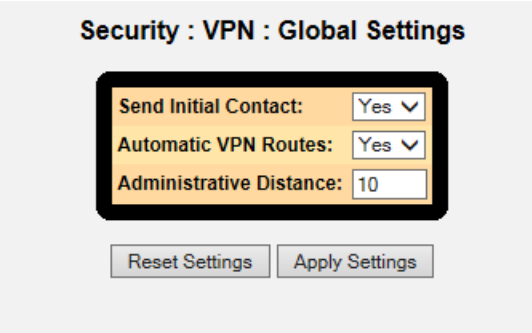
Refresh

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.

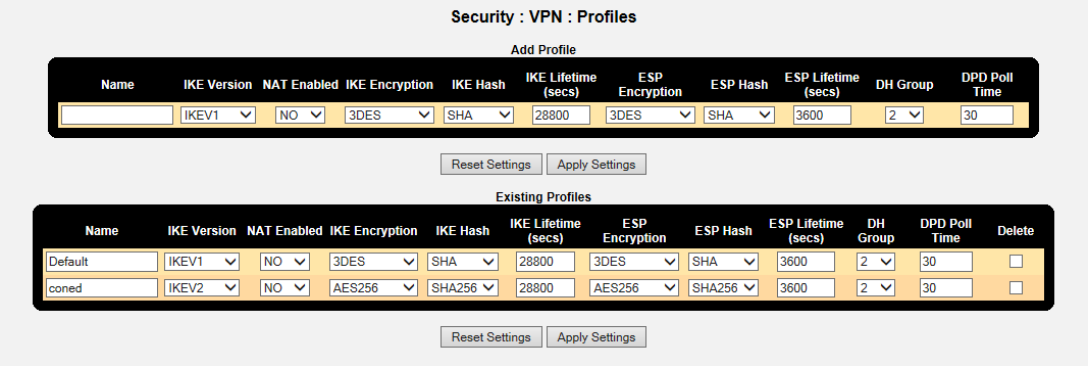


Starting with Global Settings, turn on “send initial contact”

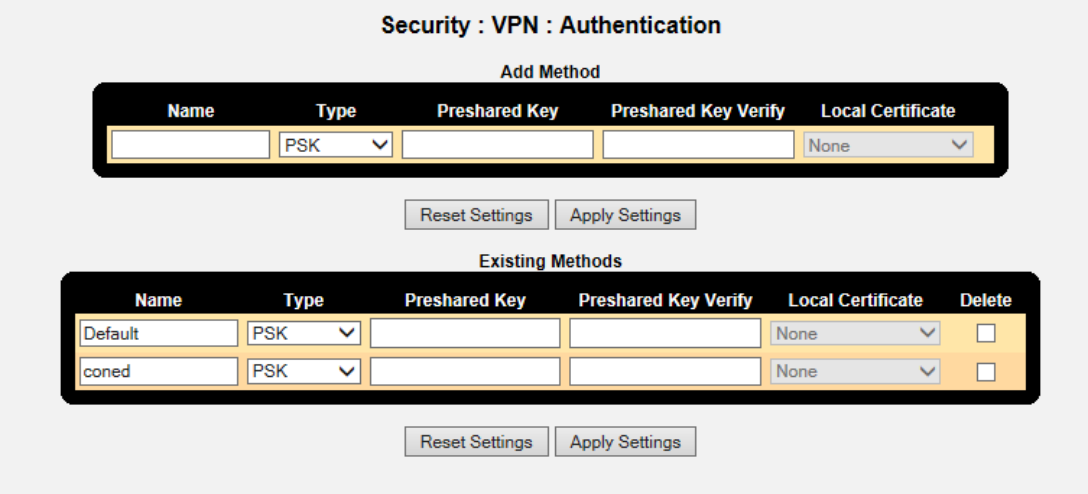


Next we build a new profile and selected the version of the IPSec VPN and the encryption settings for the Authentication and Data Transfer phases.

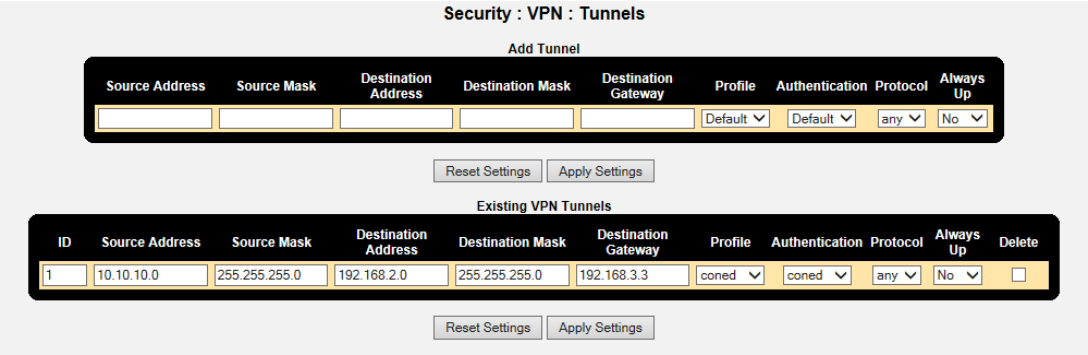
Here I selected the most secure settings, IPsec version IKEV2, AES256 encryption strength and both IKE and ESP Hash to SHA256.



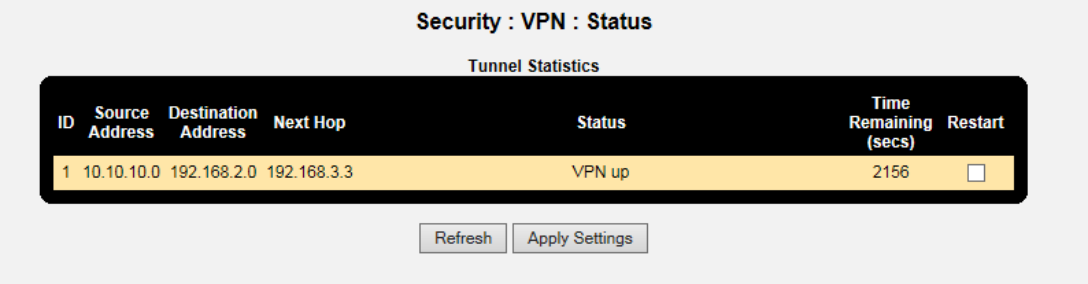
Now for the actual authentication “shared secret”, we can use Pre-Shared Key or you may prefer to build your own private certificates, not covered here. The Pre-shared Key method is just a string of characters, like a password, that is used during authentication of the 2 VPN peers. In this example it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

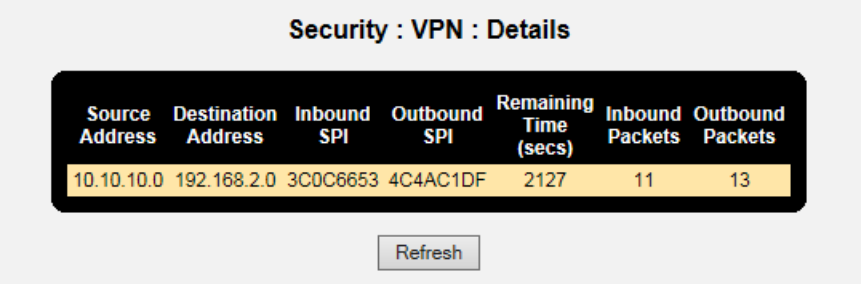


With all that set we can finally define the tunnel end points, so we want the tunnel to exist throughout the Verizon network, so in this example we want any traffic between 192.168.2.x and 10.10.10.x , ie the Control Station network and remote RTU network and be protected throughout the “public” network 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.

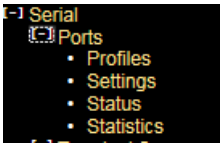


Successful VPN connection can be verified

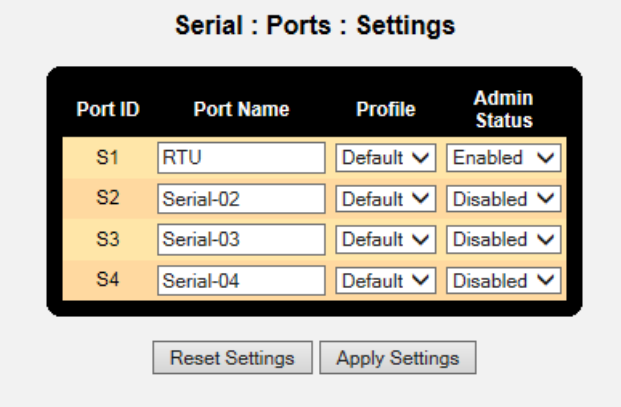




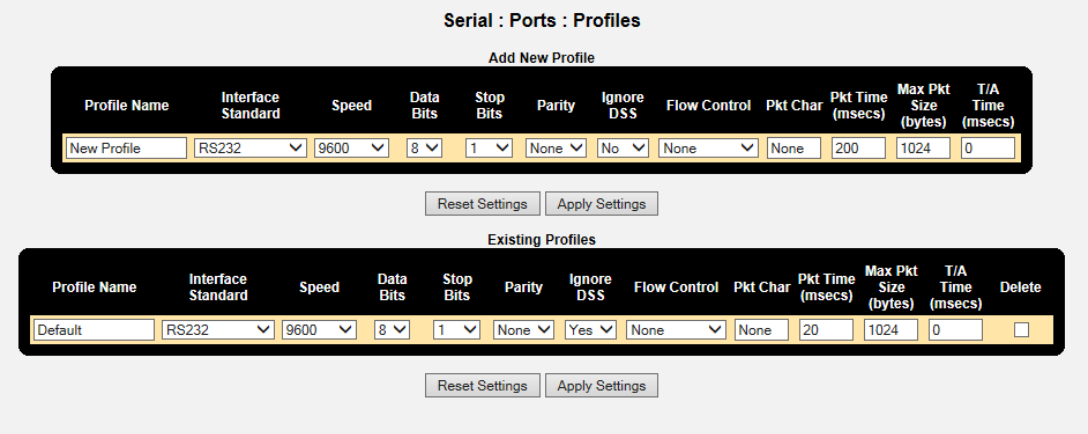
Serial Ports



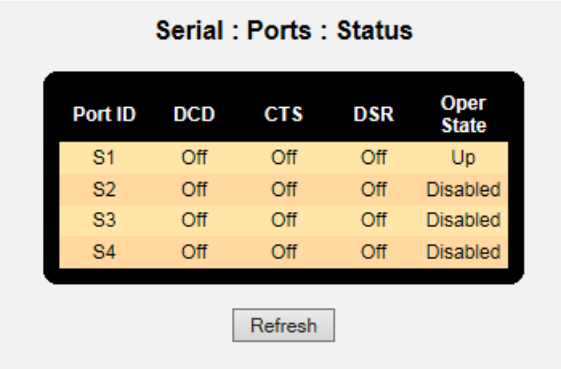
All serial ports in the default configuration are disabled, so we need to enable the port, and perhaps name it.



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.

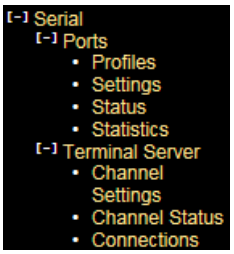


We can check the status, the Ignore DSS parameter enables the port rather than needing additional signals like DTR from the RTU.

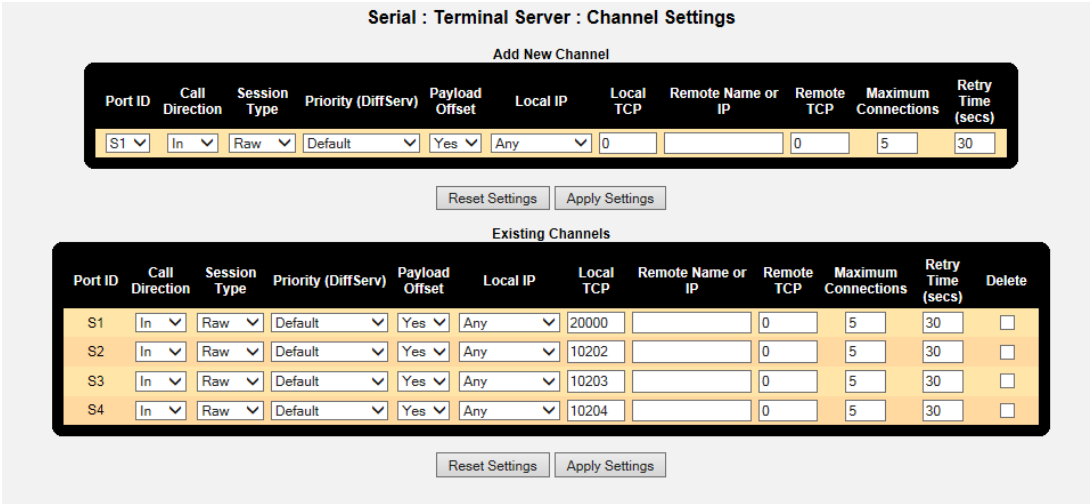


Terminal Server

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

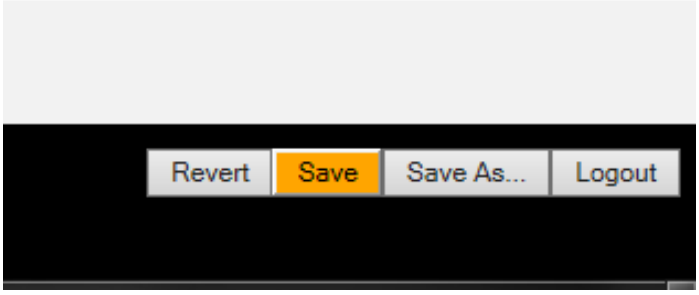


The channel settings shows call direction inbound, allows for any IP to be used, and we simply modified the listening TCP port number to match our DNP3 session, in this case 20000.



Saving Configurations

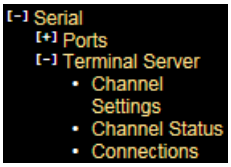
Please make sure you SAVE the configurations we have made by hitting the “SAVE” ICON at the bottom right of the WEB screen, the button is highlighted when there are configurations that have not been saved.

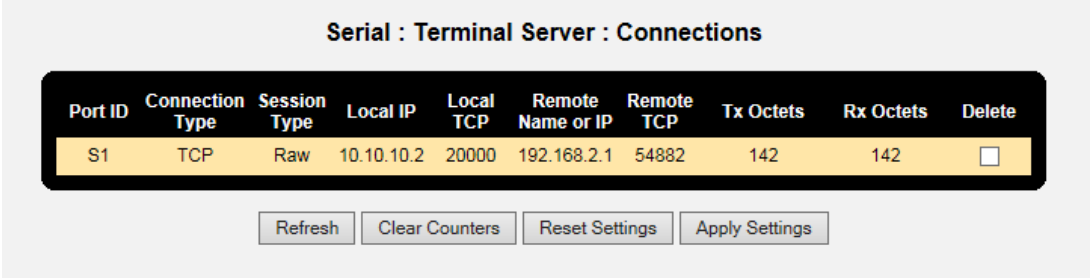


SCADA Host Connection

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





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.