

Base de conocimiento > Products > DX/10XTS Routers > DX940e - Router configuration for a SCADA application over Verizon MPLS

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.

GarrettCom	
Login ID:	1 1
Login	

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..

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
[11] Routing
[+] Q0S
[+] 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.

Port ID	Port Name	Media Typ	e	Flow Control	FEFI	Admin Status
E1	Ethernet-01	Autoneg	<	Disabled \checkmark	Disabled	Enabled 🗸
E2	Ethernet-02	Autoneg	~	Disabled \checkmark	Disabled	Disabled 🗸
E3	Ethernet-03	Autoneg	~	Disabled \checkmark	Disabled	Disabled 🗸
E4	Ethernet-04	Autoneg	~	Disabled \checkmark	Disabled	Disabled 🗸
E5	Ethernet-05	Autoneg	~	Disabled \checkmark	Disabled	Disabled \checkmark
E6	Ethernet-06	Autoneg	~	Disabled \checkmark	Disabled	Enabled 🗸

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

Ether	hernet : Bridge : Port Settings							
	Port	Bridged?						
	E1	No 🗸						
	E2	Yes 🗸						
	E3	Yes 🗸						
	E4	Yes 🗸						
	E5	Yes 🗸						
	E6	Yes 🗸						
•								
R	leset Settings	Apply Settings						

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

Default No 192.168.2.2 255.255.255.0 Image: Control of the state of th	Status	System	Remote Address	Subnet Mask	Address	DHCP?	Interface
E1 No V 192.168.3.3 255.255.0 O	Up	۲		255.255.255.0	192.168.2.2	No 🗸	Default
CELL1 No C	Up	\circ		255.255.255.0	192.168.3.3	No 🗸	E1
	Down	\bigcirc				No	CELL1
<u>Other</u>	r Option:	Oti					

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.

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 : E	BGP : Pee	er Settings			
BC Nai	GP Ne Peer IP Addr	ess Local IP Addr	ess Peer AS	Add Peer	Hold Timer Pr (sec)	ofile Inp Filt	ut Outpu er Filter	t MD5 Password
bgp-1	I 0.0.0.0	0.0.0	1	1	40 Defa	ault 🗸 NONE	E 🗸 NONE	 ✓
			Reset Setti	ings App xisting Peer	y Settings			
BGP Name	Peer IP Address	Local IP Address	Peer AS Loc	Hol al AS Tim (sec	d er Profile :)	Input Filter	Output Filter	MD5 Password Delet
bgp-1	192.168.3.2	192.168.3.3	10 20	40	Default N	NONE V	NONE 🗸	
			Reset Setti	ngs App	y Settings			

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.

		Ro	outing : BGI	P : Profiles			
			Add New I	Profile			
Profile Name	e Default Router	Redist Redis Static RIP	t Redist I OSPF	Redist Weig BGP	ht Private AS	Local Pref To Pas	CP ssive
New Profile	No 🗸	No 💙 No 🔪	✓ No ✓ []	No 💙 100	No 🗸	100 No	\checkmark
		Res	Existing P	Apply Settings			
Profile Name	Default Redi Router Stat	st Redist I ic RIP	Redist Redis OSPF BGP	t Weight	Private AS	cal Pref TCP Passive	Delete
Default	No 🗸 Yes	✓ No ✓ [No 🗸 Yes 🔪	/ 100	Yes 🗸 100	No 🗸	
		Res	set Settings	Apply Settings			

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

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
192.168.3.2	4	10	Established	2	16982	17339	No	None

And the RIB table populated with learnt IP addresses.

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	е
192.168.4.0	24	192.168.3.2	40	2	100	1	0	е

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

Route Destination	Route Mask	Next Hop	Administrative Distance	Metric	Age	Туре
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"

Send Initial Contact:	Yes 🗸
Automatic VPN Routes:	Yes 🗸
Administrative Distance:	10

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.

				Securi	ty:VPN:Pr	ofiles				
					Add Profile					
Name	IKE Versi	on NAT Enabl	ed IKE Encryptic	on IKE Hasi	h IKE Lifetime (secs)	ESP Encryption	ESP Hash	ESP Lifetime (secs)	DH Group	DPD Poll Time
	IKEV1	✓ NO ✓	3DES N	✓ SHA	28800	3DES N	SHA V	3600	2 🗸	30
				Reset Se	ttings Apply	Settings				
Name	IKE Version	NAT Enabled	IKE Encryption	Reset Se IKE Hash	Existing Profiles IKE Lifetime (secs)	ESP Encryption	ESP Hash	ESP Lifetime (secs)	DH DPD Group Tir	Poll Delete
Name	IKE Version	NAT Enabled	IKE Encryption	IKE Hash	Existing Profiles IKE Lifetime (secs) 28800	ESP Encryption 3DES	ESP Hash	ESP Lifetime (secs)	DH DPD Group Tir 2 V 30	Poll Delete
Name Default coned	IKE Version	NAT Enabled	IKE Encryption 3DES V AES256 V	Reset Se IKE Hash SHA V SHA256 V	tttings Apply Existing Profiles IKE Lifetime (secs) 28800 28800	ESP Encryption 3DES V AES256 V	ESP Hash SHA V SHA256 V	ESP Lifetime (secs) 3600 3600	DH DPD Group Tir 2 V 30 2 V 30	Poll Delete

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.

Name	Туре	Preshared Key	Preshared Key Verify	Local Certificat	te
	PSK 🗸			None	$\mathbf{\vee}$
		Reset Settings A	oply Settings		
		Existing Met	nods		
Name	Туре	Preshared Key F	reshared Key Verify	Local Certificate	Dele
Default	PSK 🗸		N	lone 🗸	
coned	PSK 🗸		Ν	lone 🗸	

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	
						Default 🗸	Default 🗸	any 🗸	No 🗸	
			-							
			L	Existing VPN T	unnels					
ID	Source Address	Source Mask	Destination Address	Reset Settings Ap Existing VPN To Destination Mask	pply Settings unnels Destination Gateway	Profile	Authentication	Protocol	Always Up	Delete
ID 1	Source Address	Source Mask 255.255.255.0	Destination Address 10.10.10.0	Reset Settings Ap Existing VPN To Destination Mask 255.255.255.0	pply Settings unnels Destination Gateway 10.10.10.2	Profile	Authentication	Protocol any V	Always Up Yes ∨	Delete

Successful VPN connection can be verified

ID	Source Address	Destination Address	Next Hop		Statu	s		Time Remaining (secs)	Restart
1	192.168.2.0	10.10.10.0	10.10.10.2		VPN (qu		2555	
			Security	: VPN : [Details	gs			
	Source Address	Destinati Addres	on Inbound s 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.

Povo	+ 9340	Save As	Logout
Rever		Save As	Logout

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..

System Name:	DX940e C
System Location:	Substation Locations
System Contact:	System Contact
System Mode:	Normal 🗸
System Prompt:	MagnumDX
TCP KeepAlive:	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 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

			WAN . FUI	t Setting	S			
Port Name	Timeslot Bandwidth	Clock	Admin Status	Mode	Time Slots	Frame Types	Line Codes	Line Build Out
WAN-01	64k 🗸	Received \checkmark	Enabled 🗸	T1 🗸	1-24	ESF (T1) 🗸	B8ZS (T1) 🗸	0to133 💊
	Port Name √AN-01	Port Name Timeslot Bandwidth NAN-01 64k V	Port Name Timeslot Clock Bandwidth Clock WAN-01 64k V Received V	Port Name Timeslot Clock Admin Bandwidth Clock Status V/AN-01 64k V Received V Enabled V	Port Name Timeslot Bandwidth Clock Admin Status Mode v/AN-01 64k v Received v Enabled v T1 v	Port Name Timeslot Bandwidth Clock Admin Status Mode Time Slots v/AN-01 64k v Received v Enabled v T1 v 1-24	Port Name Timeslot Bandwidth Clock Admin Status Mode Time Slots Frame Types v/AN-01 64k v Received v Enabled v T1 v 1-24 ESF (T1) v	Port Name Timeslot Bandwidth Clock Admin Status Mode Time Slots Frame Types Line Codes v/AN-01 64k v Received v Enabled v T1 v 1-24 ESF (T1) v B8ZS (T1) v

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.



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.

		WAN : DL	.CI Setti	ngs		
		Ado	I DLCI			_
Port II	D DLCI	CIR	IP	EEK	TYPE	
W1 🗸			Yes 🗸	None 🗸	Layer3-IP	~
		Reset Settings	Apply S	Settings		
		Existi	ng DLCIs			
Port ID	DLCI	CIR IP		EEK	TYPE	Delete
W1	100	Yes	✓ Nor	ne 🗸 Lay	er3-IP 🗸	
					Vendor St	pecific Detail
		Decet Cettings	Archie	2-11		
		Reset Settings	Apply	settings		

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 $\,$

		Routi	ing : IP Addresse	S		
Interface	DHCP?	Address	Subnet Mask	Remote Address	System	Status
Default	No 🗸 1	192.168.4.2	255.255.255.0		۲	Up
W1-DLCI 100	No 🗸 1	10.10.10.2	255.255.255.0		0	Up
CELL1	No				0	Down
					<u>Ot</u>	her Optior
	[Refresh R	Reset Settings Apply	Settings		

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.

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.

				Add Peer				
BC Nat	iP Peer IP Add	ress Local IP Add	ress Peer AS	S Local AS	Hold Timer Pro (sec)	file Input Filter	Output Filter	MD5 Password
bgp-	I 0.0.0.0	0.0.0.0	1	1 4	0 Defau	ilt 🗸 NONE		
			E	Existing Peers				
BGP Name	Peer IP Address	Local IP Address	Peer AS Lo	Hold cal AS Time (sec)	r Profile	Input Filter	Output I Filter Pas	AD5 Del sword Del
	10.10.10.1	10.10.10.2	30 40	40	Default 🗸			
FR-link								

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 : P	rofiles			
			Ad	ld New Profile	•			
Profile Nar	ne Default Router	Redist R Static	edist Re RIP OS	dist Redist SPF BGP	t Weight	Private AS	Local Pref	TCP Passive
New Profile	No 🗸	No 🗸 N	o 💙 No	✓ No ✓	100	No 🗸	100	No 🗸
		L	Ex	isting Profiles	 }			
Profile Name	Default Re Router St	dist Redist atic RIP	Redist OSPF	Redist BGP	Weight	Private AS	cal Pref Tas	CP Sive Dele
Default	No 🗸 Ye	s 🗸 No 🗸	No 🗸	Yes 🗸 10	00	Yes 🗸 100	No	~
			Reset Setti	ngs Apply	Settings			

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

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.

		I	Routing	g : 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	е
192.168.2.0	24	10.10.10.1	20	2	100	1	0	е

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

Route Destination	Route Mask	Next Hop	Administrative Distance	Metric	Age	Туре
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"

curity : VPN :	Globa	I Settir
Send Initial Conta	act:	Yes 🗸
Automatic VPN R	outes:	Yes 🗸
Administrative Di	stance:	10

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.

				Securit	y : VPN : Pi	rofiles					
					Add Profile						
Name	IKE Vers	ion NAT Enab	led IKE Encryptio	on IKE Hash	IKE Lifetim (secs)	e ESP Encryption	ESP Has	h ESP Lifetime (secs)	e DH Gro	oup DPC Ti) Poll me
	IKEV1	✓ NO ✓	3DES N	SHA N	28800	3DES Y	SHA SHA	✓ 3600	2 🗸	/ 30	
				Reset Set	tings Apply	Settings					
Name	IKE Version	NAT Enabled	IKE Encryption	Reset Set E	tings Apply xisting Profiles IKE Lifetime (secs)	ESP Encryption	ESP Hash	ESP Lifetime (secs)	DH Group	DPD Poll Time	Delet
Name Default	IKE Version	NAT Enabled	IKE Encryption	Reset Set	tings Apply xisting Profiles IKE Lifetime (secs) 28800	ESP Encryption 3DES V	ESP Hash	ESP Lifetime (secs) 3600	DH Group 2 V	DPD Poll Time	Delet
Name Default coned	IKE Version	NAT Enabled	IKE Encryption 3DES V AES256 V	Reset Set	tings Apply xisting Profiles IKE Lifetime (secs) 28800 28800	ESP Encryption 3DES V AES256 V	ESP Hash SHA V SHA256 V	ESP Lifetime (secs) 3600	DH Group 2 V 2 V	DPD Poll Time 30 30	Delet

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.

Name		T	Developed Key			6. J		
Name	PSK	Type (\			Presnared Key Ven	None	enuncau	~
			Reset Settings	Арр	ly Settings			
			Existing	Metho	ods			
Name	Тур	8	Preshared Key	Pr	eshared Key Verify	Local Certi	ficate	Dele
Default	PSK	>				None	<	
coned	PSK	$\overline{}$				None	\sim	

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 Tunne	H					
	Source Address	Source Mask	Destination Address	Destination Mask	Destination Gateway	Profile	Authentication	Protocol	Always Up	
						Default 🗸	Default 🗸	any 🗸	No 🗸	
				Reset Settings Ap	ply Settings					
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 🗸	
				Reset Settings Ap	ply Settings					

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	

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



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

Port ID	Port Name	Profile	Admin Status
S1	RTU	Default 🗸	Enabled 🗸
S2	Serial-02	Default 🗸	Disabled 🗸
S3	Serial-03	Default 🗸	Disabled \checkmark
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 : Pro	ofiles					
				Add	d New Profile						
Profile Nan	ne Interfac Standa	ce Speed	d Dat Bit	a Stop s Bits	Parity	lgnore DSS	Flow Cont	rol Pkt C	Char Pkt Tim (msecs	ne Max Pkt Size (bytes)	T/A Time (msecs)
New Profile	RS232	▶ 9600	× 8 V	/ 1 /	None 🗸	No 🗸	None	✓ Non	e 200	1024	0
			L	Exi	sting Profiles	Jounga	1				
Profile Name	Interface Standard	Speed	Data Bits	Stop Bits	Parity Igno	re S Flo	w Control	Pkt Char	Pkt Time (msecs) (t	ax Pkt T Size Ti bytes) (ms	/A ne Delet ecs)
Default	RS232 V	9600 🗸	8 🗸	1 🗸 No	one 🗸 Yes	✓ Non	e 🗸	None	20 10	024 0	
				Reset Settin	ngs Apply	Settings]				

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

Port ID	Serial : DCD	Ports :	Status	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.

Po	Port ID Call Session Priority (DiffServ) Payload Local IP Local Remote Name or Remote Maximum Time Direction Type Priority (DiffServ) Offset Local IP TCP IP TCP Connections (secs)													
S1	~	In	▼ [Raw	✓ Defaul	t	✓ Yes	s 🗸 Any	✔ 0		0		5	30
							ŀ	Reset Settings	Apply Set	tings				
								Existing C	hannels					
Port ID	Ca Direc	all tion:	Sessi Typ	ion e	Priority (Di	fServ)	Payload Offset	Local IP	Local TCP	Remote Name or IP	Remote TCP	Maximu Connecti	m Retrons Cons (sec:	y e Del s)
S1	In	~	Raw	~	Default	~	Yes 🗸	Any 🗸	20000		0	5	30	
S2	In	~	Raw	~	Default	\checkmark	Yes 🗸	Any 🗸	10202		0	5	30	
	In	~	Raw	~	Default	~	Yes 🗸	Any 🗸	10203		0	5	30	
S3								(Am)	10204		0	5	20	

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 [+] Ports [-] Terminal • Chan Settir • Chan • Conn	l Server Inel Ings Inel Status Iections								
		5	Serial : Te	ermina	Server :	Connec	tions		
Port ID	Connection Type	Session Type	Local IP	Local TCP	Remote Name or IP	Remote TCP	Tx Octets	Rx Octets	Delete
Port ID S1	Connection Type TCP	Session Type Raw	Local IP 10.10.10.2	Local TCP 20000	Remote Name or IP 192.168.2.1	Remote TCP 54882	Tx Octets 142	Rx Octets 142	Delete

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.

F	Revert	Save	Save As	Logout