

End User Manual

Model Number: M605N

Product Description: VDSL2 / ADSL2+ / Ethernet WAN Residential Gateway featuring:

Qty 4 10/100 Ethernet Ports Qty 1 Gigabit Ethernet Port Qty 1 USB 2.0 802.11b/g/n 2T2R

TABLE OF CONTENTS

SECTION 1: GUI ACCESS

	1.1	Accessing the GUI	3
SECTION 2: TROUB	LESHOOTIN	IG	
	2.1	View DHCP Statistics	5
	2.2	View ARP Statistics	6
SECTION 3: DNS CO	NFIGURAT	ION	
	3.1	Universal Static WAN DNS Addresses	7
SECTION 4: LAN CO	NFIGURAT	ION	
	4.1	Configuring LAN Services	8
	4.2	Reserving an IP Address within the DHCP Server	10
	4.3	Configuring UPnP	12
SECTION 5: NAT CO	NFIGURAT	ION	
	5.1	Configuring Port Forwarding	13
	5.2	Configuring Port Triggering	17
	5.3	Configuring the DMZ Host	21
SECTION 6: WIRELE	SS CONFIG	URATION	

SECTION 6: WIRELESS CONFIGURATION

6.1	Wireless Channel	23
6.2	Wireless SSID	23
6.3	Wireless Security	24

SECTION 1: GUI ACCESS

Section 1.1 ACCESSING THE GUI

Step 1: Accessing the GUI via a web browser

1.A Open your Web Browser

Use the modem's LAN IP Address to access the GUI locally

This is most likely http://192.168.1.254



If you are not sure what the IP Address is, you may view the gateway address assigned, via DHCP, to the NIC Card of your PC or Device.

1.B

Place the IPv4 Gateway address into the address bar of your browser.



1.C Once the modem responds, you will be challenged for a User Name and Password

	Windows Security	23
<u>ccess</u>	The server 192,168.5.254 at DSL Router requires a username and pass Warning: This server is requesting that your username and password sent in an insecure manner (basic authentication without a secure connection).	sword. d be
Username: enduser Password: password	User name	
	Password	
	Remember my credentials	
	ОК Са	ncel

1. D You will be directed to the Main GUI Page

Local Access

VisionNet			Login: admin English
Galeway QuickView	Device Info		
WAN	Board ID-	96328ann	
an Ian	Build Timoctamo	20110525 1649	
	Manufacturer:	DO Technology Inc.	
Security	ProductClass:	M505N	
Quality of Service	SeriaNumber:		
Routing	Software Version:	GAN5.CZ56T-8-DQ-R48050-US.EN	
C DNS	Bootloader (CFE) Version:	1.0.37-106.24	
Print Server	DSL PHY and Driver Version:	A2pD035a.d23c	
S Hetwork Access Storage	Wireless Driver Version:	5.60.120.11.cpe4.406	
Service Groups	This information reflects the c	urrent status of your WAN connection.	
A IPSEC			
Castinates	Line Rate - Upstream (Kbps):	0	
Contraction of the second seco	Line Rate - Downstream (Kbp	s): 0	
up Wireless	LAN IPv4 Address:	192.168.1.254	
Gateway Diagnostics	Default Gateway:		
Gateway Statistics	Primary DNS Server:	0.0.0.0	
S Management	Secondary DNS Server:	0.0.0.0	
	LAN IPv6 Address:	fe80::1	
	Default IPv6 Gateway:		
	Overview WAN		

SECTION 2: DIAGNOSTICS

Section 2.1 VIEW DHCP STATISTICS

Step 1: Access the GUI to find DHCP Statistics

1.A Select the <u>"Gateway Statistics"</u> tab located within the left-hand frameset.





This page will provide the IP Addresses assigned by the modem's DHCP server, the MAC addresses of dynamically assigned devices, and the amount of time that the device has spent on the network.

Section 2.2 VIEW ARP STATISTICS

Step 1: Access the GUI to find ARP Statistics

This step may be used to view all connected LAN devices, and is especially useful when using the "Reserve an IP Address" feature.

1.A Select the <u>"Gateway Statistics"</u> tab located within the left-hand frameset.



WHAT THESE STATISTICS MEAN:

This page will provide the MAC Addresses of all recognized devices connected to the modem. A device will only be recognized once it has requested data from the modem.

SECTION 3: DNS CONFIGURATION

Section 3.1

UNIVERSAL STATIC WAN DNS ADDRESSES

The VisionNet Modem may be assigned different DNS addresses for each WAN Service. In the event that Static IPs are to be used, you may update and change the settings with the following procedure.

Step 1: Access the GUI to find the DNS Server Page

1.A Select the <u>"DNS"</u> tab located within the left-hand frameset.

Then, In the left-hand frameset,	VisionNet VisionNet	Logen admin English
select <u>"DNS Server"</u>	 Des au 200 Des au 200 Des aux 20	too the following Static DHS IP address: Primary DHS server: Secondary DHS server:

1.B Select <u>"Use the following Static DNS IP Address"</u>

VisionNet	Login: admin English
Galeway QuickView	DRS Server Configuration
B 🔮 WAN B 💕 LAN B 🦉 Security	Select DIS Server 2/befrace from available WAW interfaces OR enter static DIS server IP addresses for the system. In ATM mode, if any a single PVC with PioA or static PVD protocial is configured, Static DIS server IP addresses must be intered. DIS Server Distributions on the multiple VAW interfaces served as spacers but only one will be used according to the priority with the first being the highest and the last one the lowest priority if the VAW interface is connected. Priority order can be changed by removing all and adding them back in again.
Banday of Service Banday Constanting Constant	OSdect DIS Server Interfaces from available WAN Interfaces: Selected DIS Server Available WAN Interfaces
9 Dertificades 9 Minutes 9 Minutes 9 Cateway Diagnostics 9 Goteway Ratisfics 9 On Management	Use the following Static DHS IP address: Primary DHS server: 10.0.0.4 Secondary DHS server: 10.0.4.4

SECTION 4: LAN CONFIGURATION

Section 4.1

CONFIGURING LAN SERVICES

Step 1: Direct Your Browser to the LAN Configuration Page

1.A Select the <u>"LAN"</u> tab located within the left-hand frameset.

Gateway QuickView	Local Area Network (LAN) Setup	
E 🔮 WAN	Configure the Broadband Router IP Address and Subnet Mask for LAN interface. GroupName Default +	
LAN IP Configuration	IP Address: 192.168.1.254 Subret Mask: 255.255.0	
E 🖌 Security	Enable IGMP Snooping	
Quality of Service		
E - A Routing		
E 💽 DN S	Enable LAN side firewall	
2 g. The Server 3 minor Access Binsge 4 minor Access Binsge 5 minor Access 5 minor Access 6 minor Access 7 minor 7 min	Deuble DHCP Server Enable DHCP Server Enable DHCP Server Start P Address: 192.164.1.84 End P Address: 192.164.1.83 Privacy US server: 0.8.0.8 Secondary DHS server: 0.8.0.8 Eased Time (four): 34 Start C P Leake Lift: (A maximum 32 entries can be configured) Edd DHCP Option Sci DHCP Advance antiat: MAC Advances: PP Address: Remerve Add Entries: Remerve Add Entries: Remerve	

Then, In the left-hand frameset, select <u>"LAN IP CONFIGURATION"</u>

2.A Configure the LAN IP Characteristics

IP Address:	192.168.1.254 (Unless your ISP has specified another address)
Subnet Mask:	255.255.255.0
Enable IGMP Snooping:	DO NOT CHANGE
DHCP Server:	Enabled
Start IP Address:	192.168.1.64
End IP Address:	192.168.1.100
Primary DNS Server:	192.168.1.254
Secondary DNS Server:	192.168.1.254 or another DNS Server
Leased Time (hour):	24
All other settings	DO NOT CHANGE
Configure Second IP Address:	DO NOT CHANGE

VisionNet						Login: adm	nin English	h •
	IP Address:	192.168.1.254						
Gateway QuickView	Subnet Mask:	255.255.255.0						
E 🍚 WAN	The second second second							
a 🦉 LAN	Enable www.sr	ooping						
LAN IP Configuration								
IPv6 LAN Config								
T Security	Enable LAN side	firevall						
	Disphis DUCD C							
B GI Walky or service	Enable DHCP S	rver						
Routing	Start IP Addres	192.168.1.64						
E 📢 DN S	End IP Address	192.168.1.253						
Print Server	Primary DNS se	rver: 192.168.1.254						
Network Access Storage	Secondary DNS	server: 8.8.8.8						
8 💑 Service Groups	Leased Time (h	our): 24						
B A IPSEC	Static IP Lease	Ust: (A maximum 32 entries	Can be configu	ned)	ast in			
Certificates	cut one	Eur Ditte	separati do	once Marance :	actority.			
- (1) Wireless	Add Entrie	s Remove Entries						
Gateway Diagnostics	-							
Gateway Statistics								
E Shanagement								
	Configure the se	ond IP Address and Subnat	Mask for LAN in	terface				
	ing configure the se	arre a record of brid dublics	Course of Long In					
				Apply/S	dVe			

2.B Select <u>"Apply / Save"</u>

RESERVING AN IP ADDRESS WITHIN THE DHCP SERVER

DEFINITION OF RESERVED IP

Some applications (Such as Port Triggering and DMZ Host) require a Static IP Address. Some devices, however, do not support Static IP Addresses or are portable in nature.

These devices may be provided a Static IP Address via the DHCP Server. When a Reserved IP Address is specified, the modem will consistently provide the same dynamic IP Address to the specified MAC Address. The Reserved IP Address will not be assigned to any other LAN Devices.

Prior to Assigning the Reserved IP Address, you must determine the MAC Address of the target LAN Device. You may copy the MAC Address from the ARP Table located within the Device Info Section of the GUI.

Step 1: Direct Your Browser to the LAN Configuration Page

1.A Select the <u>"LAN"</u> tab located within the left-hand frameset.

Then, In the left-hand frameset, select <u>"LAN IP Configuration"</u>	Constraints of the second sec	Matterns: 192.108.1.254 Matterns: 192.323.23.2.3 Image: Construction of the state	Logn admin English •
	ि 📲 Gateviay Statistics	Configure the second IP Address and Subset Mesk for LAN interface	-

1.B Select <u>"Add Entries"</u>

You will be re-directed to the "DHCP Static IP Lease" Page

Enter the MAC Address of the intended LAN Host, and the IP Address that you would like to permanently allocate to that host.

VisionNet				Login: admin	English •
Gateway QuickView	DHCP Static IP Leas	e			
🕀 🚭 WAN	Enter the Mac address	and Static IP address then click Apply/Sa	we -		
E LAN LAN IP Configuration	MAC Address: IP Address:	11:22:33:AA:BB:CC 192.168.1.201			
E 🗑 Security					
Quality of Service			Apply/Save		
Routing					
E 🤹 DN S					
Print Server					
🖲 💊 Network Access Storage					
🔊 🤗 Service Groups					
B (IPSEC					
E Gertificates					
+ 00 Wreless					
E 🔏 Gateway Diagnostics					
E 📢 Gateway Statistics					
🖲 💊 Management					

1.C Select <u>"Apply Save"</u>

Section 4.3

ENABLING UPnP

UPnP Definition

Some applications, such as the XBOX, will require UPnP for operation. UPnP will dictate how devices share information on the LAN, and the Dynamic port rules to be used for Internet Content.

Step 1: Direct Your Browser to the UPnP Page

1.A Select the <u>"Security"</u> tab located within the left-hand frameset.



1.B Select <u>"Enable UPnP"</u>



1.C Select <u>"Apply Save"</u>

SECTION 5: NAT CONFIGURATION

Section 5.1

CONFIGURING PORT FORWARDING

COMMON APPLICATIONS

XBOX:

UPnP will resolve most XBOX issues, however should you need to do further trouble-shooting the following Port Forwarding Rules may be enabled

Designation	WAN Port	LAN IP	LAN Port	Protocol
XBOX Live	88	192.168.1.230	88	TCP/UDP
XBOX Live	3074	192.168.1.230	3074	TCP/UDP

The most effective method of utilizing these rules, is to request that the end-user change the IP Address of their XBOX to the following Static IP settings:

XBOX Configuration			
IP Address Subnet Mask	192.168.1.230		
Subnet Mask	255.255.255.0		
Gateway Address	192.168.1.254		
DNS Address	192.168.1.254		

IP CAMERAS:

The following is an example of IP Camera Configuration

Designation	WAN Port	LAN IP	LAN Port	Protocol
Camera 1 6231 192.168 Camera 2 6232 192.168	192.168.1.231	80	TCP/UDP	
Camera 1 623 Camera 2 623	6232	192.168.1.232	80	TCP/UDP

The most effective method of utilizing these rules, is to request that the end-user change the IP Address of their Camera to the following Static IP settings:

IP Camera Configuration					
IP Address	192.168.1.23x				
Subnet Mask	255.255.255.0				
Gateway Address	192.168.1.254				
DNS Address	192.168.1.254				

The customer will remotely access their camera by pointing their browser to the Public IP Address of the modem, and appending the appropriate port number. (ie: 67.126.108.104:6231)

Step 1: Direct Your Browser to the Port Forwarding Configuration Page

1.A Select the <u>"Security"</u> tab located within the left-hand frameset.

	⊘ VisionNet	Login: admin English •
Then, In the left-hand frameset, select <u>"Port Forwarding"</u>	VisionNet Construction Const	Login admin WW41 side (detailine by Protocal and External port) to the Internal server with private P. add. A maximum 32 art End Protocol Internal Port Start Internal Port End Server IP Address WAR Interface Remove Interface Remove
	© Constance B (d) 00 minutes © K atomy Disputsions ⊂ M atomy Disputsions	

1.B Select the <u>"Add" Button</u>.

Please Note: If the port to be assigned is already specified in the existing Port Forwarding Table, you must remove the rule containing this port prior to creating a new one.

2.A Choose the name of the rule

Choose the appropriate WAN Interface:

If the Service you would like to have is already available in the <u>"Select a Service"</u> menu, you may select this service for autopopulation.

	🖻 🤗 Service Groups	
	B- C IPSEC	
	E Certificates	
	🖻 ښ Wireless	
You may create a custom Service	🗉 🄏 Gateway Diagnostics	
	Cateway Statistics	
by selecting "Custom Service" and	P C. Housenat	
entering a new rule name		

VisionNet									Login: admin	English	1
Gateway QuickView	NAT Virtual Serve	rs									
Orderwork Gaskies Orderwork Gaskies Orderwork Gaskies Orderwork Gaskies Orderwork Gaskies Orderwork Gaskies Orderwork Filming Orderwork Filming Orderwork Or		e, and enter the se Port End" cannol ", then "Internal of entries that ca pppoe_0_0_35/p Select One	rver IP ad be modil Port End n be conf pp0 •	fress and cl led directh ' will be set igured:32	ck "Apply/Save , Rormally, it to the same	" to forward IP is set to the s value as "Inte	packets for this ser sime value as "E ernal Port Start".	vice to the specifie sternal Port End ⁴	d server. Itowever, if you modif	v	
Algothm Algothm UPnP WAN Access Control Bindge Access Control Endge Access Control Gusality of Service	External Port Start)	External Port End	Proto	ol Inten	al Port Start	oply/Save	End				
Routing			TCP	-							
DNS			TCP	-							
Print Server	1.		TCP	-							
Natural Arrans Storage			TCP	-							
	1.1		TCP	*							
Service Groups			TCP								
Service Groups			TCP TCP	•			_				
Service Groups IPSEC Certificates			TCP TCP TCP	-							
Service Groups IPSEC Certificates Ø Wireless			TCP TCP TCP TCP	•							
Service Groups IPSEC Certificates W Wretess Sateway Diagnostics			TCP TCP TCP TCP TCP	* * * *							

ExternalUsed to access the device onPort Startthe WAN Side		
External Port End	This should be the same as "External Port Start"	
Protocol	This should be "TCP/UDP" to avoid possible errors due to end-user mis-communication	VisionNet
Internal Port Start	This should be the port that the device "listens" on (see IP Camera example)	Select the st wave selection of the sel
External Port End	This should be the same as "Internal Port Start"	- Agoom - John - Stand Canad - Stand Anna Canad - Stand of Anno Canad - Stand of Anno - Stand of Anno Canad
Remote IP	This should left blank, unless only one remote device, with a static IP, will be allowed to access this port.	S S S S S S S S S S S S S S S S S S



2.C Select "Save/Apply"

2.D Considerations

For this rule to work properly, the LAN device must have either a Static IP, or a Reserved IP

The LAN Device, and modem, may should be reset to ensure that this rule continues to work correctly

CONFIGURING PORT TRIGGERING

DEFINITION OF PORT TRIGGERING

Port Triggering is a dynamic version of Port Forwarding, in which the modem will dynamically create a temporary port forwarding rule based upon outbound activity. This is best applied for LAN devices that communicate with a remote server. Basic VPN functions are already supported by default, but some applications use non-standard communication methods.

An example would be port triggering configuration for the Nortel Contivity VPN Solution, which uses non-standard port VPN ports and requires Port Triggering to work.

The following are the port triggering rules required for Nortel Contivity VPNs.

Port Triggering for Nortel Contivity VPNs	LAN Device Outbound Port	Outbound Protocol	Port Temporarily Forwarded to Initiating LAN Device	Inbound Protocol
Port Triggering for Nortel Contivity VPNs	500	TCP/UDP	500	TCP/UDP
	10001 -	TCP/UDP	10001	TCP/UDP

In this scenario, a LAN Device (ie: The end-user's laptop) will make an outbound UDP request on ports 500 and 10001. The modem responds to this by temporarily forwarding ports 500 and 10001 to the IP address of the initiating LAN Device (ie: The end-users laptop) for the life of the session.

Port Triggering is ideal for portable devices (ie: laptops, PDAs, etc.) which require port forwarding, but for which a Static LAN IP would be antithetical to the device's common usage.

1.A Select the <u>"Security"</u> tab located within the left-hand frameset.



1.B Select the <u>"Add"</u> Button.

Please Note: If the port to be assigned is already specified in the existing Port Triggering Table, you must remove the rule containing this port prior to creating a new one.

Step 2: Configure the Port Forwarding Rule

2.A Select the appropriate WAN Interface



2.C Select "Save/Apply"

2.D Considerations

It may be difficult to determine which ports must be used for a particular application. It is best to specify the LAN device as the DMZ host to see if this resolves the issue.

If this does not resolve the issue, the port triggering rule should be removed and replaced with port forwarding. Once port forwarding has been verified to work then port triggering may be re-visited. If port triggering does not work, then further research should be done to identify the behavior of the communication between the LAN device and the Server.

CONFIGURING THE DMZ HOST

DEFINITION OF DMZ Host

In the event that a remote application attempts to communicate via an inactive, or unspecified, port; the port will be dynamically forwarded to the IP Address specified as the DMZ Host.

If a specific device is to be assigned as a DMZ host, this device should have either a Static IP or a Reserved IP.

Step 1: Direct Your Browser to the DMZ Host Configuration Page

1.A Select the <u>"Security"</u> tab located within the left-hand frameset.

	VisionNet	Login admini English •
	Gateway GuickView	NAT DNZ Host
	E 🕒 WAN	The Broadband Router will forward IP packets from the WAII that do not belong to any of the applications configured in the Virtual Servers table to the DM2 host computer.
	E 🖌 Security	Enter the computer's IP address and click 'Apply' to activate the DM2 host.
Then, In the left-hand frameset,		Clear the IP address field and click 'Apply' to deactivate the DMZ host.
select "DM7 Host"	And frameset,	
Select DIVIZ HOST	Post Triggering Multi Net GAZ Hes GAZ Hes UPAP UPAP UPAP WAN Asses Control Gridge Asses Control Gridge Asses Control	Aqpty/Save
	E Quality of Service	
	E Reuting	
	E 🔍 DNS	
	e an Print Server	
	🗉 🗞 Network Access Storage	
	E 😤 Service Groups	
	B (PSEC	
	🕀 🎑 Certificates	
	🖹 👘 Wireless	
	Cateway Diagnostics	
	Cateway Statistics	
	T C House and	

1.B Enter the desired DMZ Host IP Address



1.C Select the <u>"Save/Apply"</u> Button.

SECTION 6: WIRELESS CONFIGURATION

Section 6.1

CHANGING THE WIRELESS CHANNEL

When to change the Wireless Channel.

Many items in your home, and your immediate neighbors' homes, likely use the 2.4 Ghz range. There are 11 possible channels that may be used within this spectrum. If your wireless connection becomes very slow, or drops, there may be other devices that are impeding upon your network. This is when you should consider changing your wireless channel.

Step 1: Direct Your Browser to the Global Wireless Configuration Page

Then, In the left-hand frameset, select <u>"Global Settings"</u>

1.A Select the <u>"Wireless"</u> tab located within the left-hand frameset.

Control of the second set				
VisionNet			Login enduser English	•
Control Carlos Control Carlos Control Carlos Control Carlos Control Control				
E 😻 Security	Rand-	24GHs *		
E CNS	Channel:	1 .	Current: 1 (interference: acceptable)	
T an Print Server	Auto Channel Timer(min)	a -		
	802.11n/EWC:	Auto +		
Network Access Storage	Bandwidth:	20MHz in 2.4G Eland	and 40MHz in 5G Band + Current: 20MHz	
IPSEC	Control Sideband:	Lower +	Current: None	
- 0:0 Wireless	802.11n Rate:	Amo +		
SSID	802.11n Protection:	Auto *		
Security Settings	Support 802,11n Client Only:	07 +		
MAC Filtering	RIFS Advertisement:	- III		
Globel Settings	DBSS Co-Existance:	Disable =		
E Category Discovering	RX Chain Power Save:	Enable +		
A contract of the second	RX Chain Power Save Quiet	10		
Cateway Statistics	RY Chain Devicer Save PPC			
E 💊 Management	Padio Poular Save	Deatin +		
	Radio Power Save Outet Time:	(0		
	Padio Power Casis PPC-	10		
	Radio Forrer Save (13,	10		
	Kablo Power Save On Time:	3.6.80		
	Dig Kate:	Auto w		
	manucos note:	Auto		

1.B Enter the desired Channel.

1, 6, and 11 tend to operate the best.

Other Channels to consider are 3 and 9.

Once you have selected the new channel, select "Save/Apply" at the bottom of the screen.

192.168.1.254		,D +	BCX ODS Router	n * 1
VisionNet				Login: enduser English •
 Gatevary QuickView WAN LAN 	Wireless Advanced This page allows you to configurate to a particular speed, set t the access point, set XPress me Click 'Apply/Save' to configure t	ire advanced features of the frogmentation thresh ode and set whether sho the advanced wireless o	the wireless LAN interface. You can select a particular old, set the RTS threshold, set the weikeup intervel for rt or long preambles are used. ptions.	hannel on which to operate, force the transmission lents in power-save mode, set the beacon interval for
E V Security	Band:	2.4GHz *		
🕀 🍓 DNS	Channel:	1 .	Current: 1 (interference: acceptable)	
T an Print Server	Auto Channel Timer(min)	a		
+ 💊 Network Access Storage	802.11n/EWC: Bandwidth:	Auto *	nd JBMHz in 5G Band + Current: 20MHz	
E DIPSEC	Control Sideband:	Lewest +	Current: None	
- 0.0 Wireless	802.11n Rate:	Ano +		
SSID	802.11n Protection:	Auto *		
Security Settings	Support 802.11n Client Only:	0# +1		
ALAC Filtering	RIFS Advertisement:	0.00 +		
With Bridging	OBSS Co-Existance:	Disable =		
	RX Chain Power Save:	Enable +		
Gateway Diagnostics	RX Chain Power Save Quiet			
Gateway Statistics	Time:			
1 😪 Management				
	Radio Power Save:	L/ISBDIE +		
	Radio Power Save Quet Time:	10		
	Radio Power Save PPS:	10		
	Radio Power Save On Time:	50		
	54g Kate:	(MDps *		
	Mulucast Rate:	Augo *		
	Basic Kate:	DetBru	7	

1.C Select the <u>"Save/Apply"</u> Button.

CHANGING THE WIRELESS SSID

When to change the Wireless SSID

You may wish to broadcast a different network name than the one provided.

Step 1: Direct Your Browser to the SSID Configuration Page

1.A Select the <u>"Wireless"</u> tab located within the left-hand frameset.



1.B Enter the new SSID Name

select <u>"SSID"</u>

The following should be enabled:

Enabled Wireless

Disable WMM Advertise

Enable Wireless Multicast Forwarding

Once you have entered the SSID Information, select "Save/Apply" at the bottom of the screen.

VisionNet				Login: enduser	English	•
Gateway QuickView	Wireless	Basic				
E 🍚 WAN	This page all scans, set th Click 'Apply/	ows you to configure basic features of the wirele a wireless network name (also known as SSID) a ave' to configure the basic wireless options.	ss LAN interface. You can enable or disa ind restrict the channel set based on cos	ble the wireless LAN interface, hide the network from ac intry requirements.	ive.	
Security Security Security Security Plots haves Security Plots Plots Plots Security Plots Security Security	☑ Enable ☐ Hide, ☐ Cleans ☑ Enable SSID; BSSID; BSSID; Country; Max Clients	e Wireless Kocess Peint Stelejeion ie WMM Advertise Wireless Multicast Forwarding (WMF) Valcenter P4:SE-IP7962:SE-IZ7 LIM/TED STATES 18				
t 💊 Management	Apply/Sa	a				

1.C Select the <u>"Save/Apply"</u> Button.

CHANGING THE WIRELESS ENCRYPTION

When to change the Wireless Encryption

You may wish to use a special login password for your wireless network.

NEVER LEAVE YOUR NETWORK UNENCRYPTED!!! THIS IS VERY INSECURE AND COULD RESULT IN LEGAL TROUBLE SHOULD AN UNAUTHORIZED USER USES YOUR NETWORK FOR ILLEGAL ACTIVITY!

Step 1: Direct Your Browser to the Security Settings Page

Then, In the left-hand frameset, select <u>"Security Settings"</u>

1.A Select the <u>"Wireless"</u> tab located within the left-hand frameset.

		-				
VisionNet				Login: enduser	English	•
Cateway QuickView	Wireless Security					
	This page allows you to canfi You may setup configuration through WFF Protected Setup Desire WPS Enable WPS Manual Setup AP You can set the rehowed suff see 47 whether a rehows the	gure security features of th manually (WPS) Disabled • entication method, select d v is required to authenticat	e wireless UAI interface.			
	Click 'Apply/Save' when done					
- Global Settings	Select SSID:	NewSSIDName100 -				
Gateway Diagnostics	Network Authentication:	WPA2-PSK	2			
🕆 💊 Management	WPA/WAPI passphrase:	*******	Click here to display			
	WPA Group Rekey Interval:	0				
	WPA/WAPI Encryption:	TKIP+AES -				
	WEP Encryption:	Apply/Save				

1.B Under "Manual Setup AP"



1.C Select the <u>"Click Here to Display"</u> Button; and verify your encryption key.

1.D Select the <u>"Save/Apply"</u> Button.

FCC Information

This equipment complies with CFR 47, Part 15.19 of the FCC rules. Operation of the equipment is subject to the following conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received; including interference that may cause undesired operation.

This device must not be co-located or operating in conjunction with any other antenna or transmitter

NOTE: THE MANUFACTURER IS NOT RESPONSIBLE FOR ANY RADIO OR TV INTERFERENCE CAUSED BY UNAUTHORIZED MODIFICATIONS TO THIS EQUIPMENT. SUCH MODIFICATIONS COULD VOID THE USER'S AUTHORITY TO OPERATE THE EQUIPMENT.

Federal Communications Commission (FCC) Requirements, Part 15

This equipment has been tested and found to comply with the limits for a class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation.

This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

---Reorient or relocate the receiving antenna.

---Increase the separation between the equipment and receiver.

---Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.

---Consult the dealer or an experienced radio/TV technician for help.

Regulatory information / Disclaimers

Installation and use of this Wireless LAN device must be in strict accordance with the instructions included in the user documentation provided with the product. Any changes or modifications (including the antennas) made to this device that are not expressly approved by the manufacturer may void the user's authority to operate the equipment. The manufacturer is not responsible for any radio or television interference caused by unauthorized modification of this device, or the substitution of the connecting cables and equipment other than manufacturer specified. It is the responsibility of the user to correct any interference caused by such unauthorized modification, substitution or attachment. Manufacturer and its authorized resellers or distributors will assume no liability for any damage or violation of government

CAUTION: To maintain compliance with FCC's RF exposure guidelines, this equipment should be installed and operated with minimum distance 20cm between the radiator and your body. Use on the supplied antenna. Unauthorized antenna, modification, or attachments could damage the transmitter and may violate FCC regulations.

MPE Statement (Safety Information)

Your device contains a low power transmitter. When device is transmitted it sends out Radio Frequency (RF) signal.

Safety Information

In order to maintain compliance with the FCC RF exposure guidelines, this equipment should be installed and operated with minimum distance 20cm between the radiator and your body. Use only with supplied antenna. Unauthorized antenna, modification, or attachments could damage the transmitter and may violate FCC regulations.

FCC Part 68 Statement

This equipment complies with part 68 of the FCC rules. On the rear panel of this equipment is a label that contains, among other information, the FCC registration number and ringer equivalence number (REN) for the equipment. If requested, this information must be provided to the telephone company. The REN is used to determine the quantity of devices which may be connected to the telephone line. Excessive RENs on the telephone line may result in the devices not ringing in response to an incoming call. In most, but not all areas, the sum of the RENs should not exceed five (5.0). To be certain of the number of devices that may be connected to the line, as determined by the total RENs, contact the telephone company to determine the maximum REN for the calling area. This equipment uses the following USOC jack: RJC. An FCC-compliant telephone cord and modular plug is provided with this equipment. This equipment is designed to be connected to the telephone network or premises wiring using a compatible modular jack which is Part 68 compliant.

This equipment cannot be used on telephone company-provided coin services. Connection to Party Line Service is subject to state tariffs. If this equipment causes harm to the telephone network, the telephone company will notify you in advance that the temporary discontinuance of services may be required. If advance notice isn't practical, the telephone company will notify the customer as soon as possible. Also, you will be advised of your right to file a compliant with the FCC if you believe it is necessary. The telephone company may make changes in its facilities, equipment, operations, or procedures that could affect the operation of the equipment. If this happens, the telephone company will provide advance notice in order to maintain uninterrupted service. If the trouble is causing harm to the telephone system, the telephone company may request that you remove the equipment from the network until the problem is resolved. It is recommended that the customer install an AC surge arrestor in the AC outlet to which this device is connected. This is to avoid damaging the equipment by loca lightning strikes and other electrical surges.