

If you clicked Add, the following screen will be displayed. Click Create.

User Guide

Edit <u>V</u> iew Favorites ]	<u>r</u> ools <u>H</u> elp	internet Explorer				
vei	ri <mark>zon</mark>					
Main	Wireless Settings	My Network	Firewall Settings	Advanced	System Monitoring	
Main Port Forwarding		Follow th	New Port Forward	ing Rule		
		1. Select an existing Service	/ Rule or create a new of	ne		
		2. Select how the service will	Create	Edit	Delete	
		• Host	Allows unsolicited inbound	d traffic to a particular PC on	the LAN.	
		Opynamic	Enables inbound traffic ba	ased on specific outbound tra	ffic.	
		3. For Hosted Service, Select	a PC on the LAN			
		Select a Discovered LAN device:	SALLE-XP2 🗸	Or manually enter a LAN IP:	192.168.1.18	
			Apply Car	ncel		
						Tabasat

If you clicked **Create**, the following **Create Port Forwarding Service** screen will appear. Using this screen, you can create port forwarding and port triggering services for your Router. The following sections explain how to customize these services in your Router.

- **Port Forwarding Ranges of Ports**: This option allows you to forward a range of WAN ports to an IP address on the LAN.
- **Trigger Ports:** This option allows you to forward a range of ports to an IP address on the LAN only after specific outbound traffic.

http://10.16.90.10:2420 - Ble Edit View Figvorites To	Yerizon - Microsoft Internet ∋is ⊟elp	Explorer					ED
veri	70n						
Main	Wireless Settings	Wy Network	Firewall Settings	Advanced		System Monitoring	
Main			Create Port Forw	arding Service			
Port Forwarding		Follow the st	eps below to define a nev	custom port forwarding	service.		
	1. Enter a nam	e for the custom se	ervice :				
	2. Specify the p Port Forwar	ort forwarding ent	<b>ry based on your spec</b> t Trippering	ific ports:			
	3. Define the fi	rst rule:					
	Protocol	Iobal PortStart	Global PortEnd	Base HostPort	Direction	Port Direction	
			Apply	Cancel	n V		
Done							Internet



User Guide

VersaLink Wireless Gateway (Model 7500)

### 15.3.3.3.1 Creating a Service Based on Specific Port Forwarding Ports

The Port Forwarding feature allows you to forward a range of WAN ports to an IP address on the LAN. You can set up a port forwarding entry based on your specific ports.

**IMPORTANT:** Using various Internet applications depends on the Router's firewall settings. Make sure that the Router's firewall is set to Medium Security or lower to take advantage of all the port forwarding features. Firewall settings take precedence over port forwarding services configured in the Router. For example, if the firewall is set to Medium Security, this will block ICMP packets even if the ICMP service is enabled. If a port forwarding service is not working, try setting the firewall to a lower setting.

To create a port forwarding service based on specific port forwarding ports, at the **Create Port Forwarding Service** screen, do the following:

- 1. Type the name of the custom service that you are creating in the field provided. This will be the name of the port forwarding service for which you are configuring specific Port Forwarding rules.
- 2. Click the Port Forwarding option.
- 3. Select the desired protocol from the **Protocol** drop-down menu.
- 4. Enter the desired Global Port Start, Global Port End, and Base Host Port values in the fields provided, as shown in the example below.
- 5. Select the desired direction settings
- 6. Click Apply to allow the changes to take effect.

**NOTE:** If you clicked **Cancel** in the **Create Port Forwarding Service** screen, the service you created will be displayed; however, it will not be activated in your Router. You must click **Apply** to allow the settings to take effect.

http://10.16.90.10:2420 - Ve Elle Edit Vew Favorites Ioo	erizon - Microsoft Inter Is Help	net Explorer					
veri	on						
Main	Wireless Settings	My Network	Firewall Settings	Advanced		System Monitoring	
Main Port Forwarding		Follow the st	Create Port Forw	arding Service	service.		
	1. Enter a n First Port Forwa	ame for the custom se	ervice :				
	2. Specify t Port Fo	<b>he port forwarding en</b> warding O Por	<b>try based on your spe</b> o t Triggering	ific ports:			
	3. Define th	e first rule:					
	Protocol	Global PortStart	Global PortEnd	Base HostPort	Direction	Port Direction	
	tcp 💌	22	24	23	h 💙	Dst 😕	
			Appiy	Cancel			
							🔮 Internet



User Guide

VersaLink Wireless Gateway (Model 7500)

	Port Forwarding Service
Drotocol	TCP – Transmission Control Protocol
PIOLOCOI	UDP – User Datagram Protocol
Global Port Start	The WAN-side TCP/UDP start port.
Global Port End	The WAN-side TCP/UDP end port.
Base Host Port	The port on the WAN that will host the port forwarding service selected. Base Host Port is
	the first port that will be used for a specific service when configured for a range of ports.
Direction/	The port direction for the port forwarding rule.
Port Directon	

If you clicked **Apply**, the following **Service Details** screen will be displayed. Click **Done**.

ver	i on		1.1-	0	F		
Main	Wireless Settings	My Network	Firewall Settings	Advanced	Syst Monite	em oring	
Port Forwarding		Service Type	Name First Port Port Forw	Forwarding Ser arding	vice		
	Entry	Protocol	Global Port Start	Global Port End	Base Host Port	Action	
	Add	tcp	22	24	23	<b>*</b>	

7. Return to the **New Port Forwarding Rule** screen and, from the drop-down menu, select the name of the custom service that you created (the name should appear at the bottom of the list under **Custom Defined Service**).

http://10.16.90.10:2420 - \	Verizon - Microsol	it Internet Explorer					
Veri Hain	i on Wireless Settings	Hy Network	5 Firewall			System Monitoring	
Main Port Forwarding		Folk	New Port Fo	rwarding Rul	e your device.		
		1. Select an existing Serv	ice / Rule or create a	new one			
		Custom Defined Service Peasl/udo Return To Castle Wolfenstein Reger Wite Sersion Natation Protocol (SIP) Sourcest Server SIP ALG Soriner Rade,/Netscape Music SSIH Secure Shell Barroat Darliet Command	be activated Allows unsolicite Enables inbound	d inbound traffic to traffic based on sp	a particular Po recific outbound	C on the LAN.	
		SU/30FII Teinet Teinet Tenes Usen Sun & Dune 2000 Tritee2 Utmeal Townament Server USENET News Service VWC Wetwood Online, C&C Workd Wide Web (HTTP) Jacob Live	a PC on the LAN SALLEXP2 Apply	Or manua     Cancel	elly enter a LAN	4 IP: 192.168.1.18	
		Yahoo Messenger Phone Custom Defined Service Find Post Forwarding Service Triggering Rule					
lone							Sinternet



User Guide

*VersaLink Wireless Gateway (Model 7500)* This screen displays the service name in the field.

http://10.16.90.10:2420 - Ver Ele Edit Vew Favorites Tools	rizon - Microso Help	oft Internet Explorer				
veri	on IIII		55		<b>E</b>	
Main	Wireless Settings	My Network	Firewall Settings	Advanced	System Monitoring	
Main Port Forwarding		Follow th	New Port Forwar	rding Rule service on your device.		
		1. Select an existing Service ;				
		First Port Forwarding Service	Create	Edit	Delete	
		2. Select how the service will	be activated			
		() Host	Allows unsolicited inbox	and traffic to a particular PC or	the LAN.	
		Opynamic	Enables inbound traffic	based on specific outbound tra	affic.	
		Select a Discovered LAN device:	SALLE-XP2	Or manually enter a LAN IP	192.168.1.18	
			Annha			
			Appry C			
						Internet

- 8. Select how the service will be activated.
  - Host allows unsolicited inbound traffic to a particular PC on the LAN.
  - Dynamic enables inbound traffic based on specific outbound traffic.
- 9. Select the IP address of the device that will host the service (select a device from the Select a Discovered LAN device drop-down menu or type an IP address in the field provided).
- 10. Click **Apply** to allow the service to be added to the Router's list of active services.



User Guide

If you clicked **Apply**, the following screen will appear. The Port Forwarding service has been added to the list of active services. To add additional port forwarding services to your Router, repeat steps 1 through 10.

🗟 http://10.16.90.10:2420 - Ver	izon - Microsoft Internet Explorer				
Ele Edit View Favorites Tools	Help				At 1
Veri Main	OII Wireless Settings Hy Netwo	rk Settir	ali Advan	ced System Monitoring	
Main General Port Forwarding DM2 Host Remote Administration Static NAT	This feature enables appl compu Current Profile: Default 🗸	Port ications(Games, Webcam iters and a specific device New	Erorwarding s, IM & Others) by opening a port inside your local area r	tunnel between remote(internet) etwork(LAN),	
Security Log	Name	Mode	Host Device	Action	
	First Port Forwarding Service	Port Forwarding	192.168.1.18	🚽 😽	
	IPSEC ALG	Port Forwarding	Dynamic	🚽 🙀	
	Add			<b>2</b>	
			Close		
🙋 Done					🔮 Internet

To view the details for the service, click the details icon in the **Action** field. The following screen will appear. Click **Close** to return to the **Port Forwarding** screen.

http://10.16.90.10:2420 -	Verizon - Microsoft Interr	net Explorer					
<u>File Edit View Favorites T</u>	<u>F</u> ools <u>H</u> elp						
ver	ri <mark>zon</mark>						
	(in)		Lte				
	Wireless		Firewall		Svet	em	
Main	Settings	My Network	Settings	Advanced	Monito	oring	
Main			Service De	tails			
Port Forwarding							
L.		Service	Name First Port Port Forw	Forwarding Ser arding	vice		
	Entry	Protocol	Global Port Start	Global Port End	Base Host Port	Action	
	1	tcp	22	24	23	<b>×</b>	
	Add					<b>EX</b>	
			Close				
Done							🥑 Internet



### 15.3.3.3.2 Creating a Service Based on Specific Port Triggering Ports

The Trigger Ports feature allows you to forward a range of ports to an IP address on the LAN only after specific outbound traffic. You can set up a port triggering entry based on your specific ports.

**IMPORTANT:** Using various Internet applications depends on the Router's firewall settings. Make sure that the Router's firewall is set to Medium Security or lower to take advantage of all the port forwarding features. Firewall settings take precedence over port forwarding services configured in the Router. For example, if the firewall is set to Medium Security, this will block ICMP packets even if the ICMP service is enabled. If a port forwarding service is not working, try setting the firewall to a lower setting.

To create a port forwarding service based on specific port triggering ports, at the **New Port Forwarding Rule** screen, click **Create**.

http://10.16.90.10:2420 - Veri	zon - Microso	ft Internet Explorer							
le Edit View Favorites Tools	Help								
veriz	on								
					3				
Contraction of the second	Wireless		Firewall		System				
Main	Settings	My Network	Settings	Advanced	Monitoring				
-									
Main			Sector Sector Sector						
			New Port Forwar	ding Rule					
Port Forwarding		Follow the steps below to set up a service on your device.							
	1	1. Select an existing Service / Bule or seasts a new and							
		1. Select an existing Service	/ Rule or create a new	one					
		Select A Service / Rule	Create	Edit	Delete				
		2. Select how the service will	be activated						
		• Host	Allows unsolicited inbou	nd traffic to a particular PC o	in the LAN.				
		Opynamic	Enables inbound traffic	based on specific outbound tr	raffic.				
		3. For Hosted Service, Select	a PC on the LAN						
		Select a Discovered LAN device:	SALLE-XP2 🔽	Or manually enter a LAN IF	P: 192.168.1.18				
			Apply C	ancel					
e						Internet			

User Guide



User Guide

If you clicked **Create** in the preceding screen, the following screen will appear. Complete the following steps to add a port triggering rule.

1. Click the **Port Triggering** option. (By factory default, the **Port Forwarding** option will be selected.)

a http://10.16.90.10:2420 -	Verizon - Microsoft Inter	net Explorer						
Ele Edit View Favorites I	pols <u>H</u> elp							<u>A</u> *
ver	i <mark>r on</mark>						_	
	(in)		Lte	R				
	Wireless	25	Eirewall			System		
Main	Settings	My Network	Settings	Advanced		Monitoring		
Main	0. Vertion - Microsoft Internet Laplorst         : joid Bdp             Prior Bdp             Wireless             Wireless           Wireless           Wireless       Hy Network       Firewall       Statem       Nontoring       Create Port Forwarding Service       Follow the steps below to define a new custom port forwarding service.       I Enter a name for the custom service :       Port Forwarding       Port Triggering       3. Define the first rule:       Protocol       Global PortEnd       Base HostPort       Direction       Port Clowarding       Aggy       Cancel							
Port Forwarding		Follow the st	eps below to define a new	custom port forwarding	service.			
	1. Enter a n	ame for the custom se	rvice :					
			]					
	2.6			6t				
	2. Specify th	e port forwarding ent	ry based on your speci	nc ports:				
	O Port For	warding O Port	rnggenng					
	3. Define th	a first rule:						
	Protocol	Global PortStart	Global PortEnd	Base HostPort	Direction	Port Direction		
	top 💌				ln 💌	Det 🖂		
			Apply	Cancel				
() and								8
E Done							internet	-

If you clicked the **Port Triggering** option in the preceding screen, the following **Create Port Triggering Rule** screen will be displayed.

http://10.16.90.10:24	20 - Verizon - Microsoft In	iternet Explorer						- 2
Ele Edit Vew Favorites	Iools Help							4
								1
V	erizon							
	(10)				~			
E B	2		2	5	3			
Main	Wireless	My Network	Firew Settin	all	Advanced	System		
L	Settings		betti	<b>.</b>		Homeonity	,	
			Create Port Tr	agering Rule				
Main			creater on the	ggening here				
Port Forwarding								
	1. Enter a name for t							
	2. Specify the port tri	iggering rule based	on your specific por	ts:				
	O Port Forwarding	<ul> <li>Port Trigger</li> </ul>	ing					
	3. Define the first rul	e:						
	Global Port Start	Global Port End	Local Port Start	Local Port End	IncomingProtocol	OutGoingProtocol		
					top 💌	top 💌		
	When outbound traffic	the range of	Global' Ports	ng is enabled through				
			Apply	Cancel				
							a tatanat	



- 2. Type the name of the custom service that you are creating in the field provided. This will be the name of the port forwarding service for which you are configuring specific Port Triggering rules.
- 3. Enter the desired Global Port Start, Global Port End, Local Port Start, and Local Port End values in the fields provided, as shown in the example below.
- 4. Select the desired Incoming and Outgoing protocol for the rule.
- 5. Click **Apply** to allow the changes to take effect.

**NOTE:** If you clicked **Cancel** in the **Create Port Triggering Service** screen, the values you entered will be displayed; however, they will not be active in your Router. You must click **Apply** to allow the settings to take effect.

verizon							
n Wireless Settings	My Networ	k Fire Setti	wall ngs	Advanced	System Monitoring		
		Create Port Tr	iggering Rule				
ng	Follow t	the steps below to defin	ne a new port triggering	g rule.			
1. Enter a name fo	r the port triggering r	ule :					
First Port Triggering Servi	First Port Triggering Service						
2. Specify the port O Port Forwarding	triggering rule based	on your specific poo	rts:				
3. Define the first	rule:	1					
Global Port Start	Global Port End	Local Port Start	Local Port End	IncomingProtocol	OutGoingProtocol		
When outbound traf	ic is detected in the 'Trig the range of	ger' Port, Port Forward 'Global' Ports Apply	ing is enabled through Cancel				

	Port Triggering Service				
Global Port Start	The WAN side TCP/UDP start port.				
Global Port End	The WAN side TCP/UDP end port.				
Local Port Start	The local LAN side TCP/UDP start port.				
Local Port End	The local LAN side TCP/UDP end port.				
Incoming Protocol	The protocol to use for inbound traffic.				
Outgoing Protocol	The protocol to use for outbound traffic.				



User Guide

- 6. After you click **Apply**, the following screen will be displayed. From the drop-down list, select name of your custom port triggering rule (the name will appear at the bottom of the list under **Triggering Rule**).
- 7. Click Apply to allow the service to be added to the Router's list of active services.

http://10.16.90.10:2420 - V	/erizon - Microsoft	t Internet Explorer				
Eile Edit View Favorites Ion	ols <u>H</u> elp					
Veri Main	Vireless Settings	My Network	Firewall Settings	Advanced	System Monitoring	
Main Port Forwarding		Follo	New Port Forward	ding Rule		
		1. Select an existing Servi	ice / Rule or create a new o	one		
		Select A Service / Rule Return To Castle Wolfenstein Roger Wilco Session Initiation Protocol (SIP) ShoutCast Server SIP ALG Spinner Radio/Netscape Music SSH Secure Shell Starcraft Starfielt Command SoF/SOFII Teinet Sun & Dune 2000 Tribes2 Utima Online Unreal Toumament Server USENET News Service VNC Westwood Online, C&C Word Wide Web (HTTP) Xbox Live Yahoo Messenger Chat Yahoo Messenger Phone Custom Defined Service First Port Forwarding Service Triggering Rule	Create C	Edit nd traffic to a particular PC on pased on specific outbound tra Or manually enter a LAN IP:	Delete the LAN. ffic.	
e		hist rolt higgeling service				Internet

If you click **Apply**, the following pop-up screen will appear. Click **OK** to continue.





User Guide

If you click **OK** in the pop-up screen, the following screen will appear. The Port Triggering service has been added to the list of active services. To add additional port triggering services to your Router, repeat steps 1 through 7.

🕙 http://10.16.90.10:2420 - V	/erizon - Microsoft Internet Explorer				
Eile Edit View Favorites Too	ols <u>H</u> elp				
Veri Main	ON Wireless Settings My Net	work Fire	wall Ings Advan	ced System Monitoring	
Main General Port Forwarding DMZ Host Remote Administration Static NAT	This feature enables ar con Current Profile: Default	Po pplications(Games, Webca pputers and a specific devi v	rt Forwarding ms, IM & Others) by opening a ce port inside your local area r w Edit	tunnel between remote(Internet) hetwork(LAN).	
Security Log	Name	Mode	Host Device	Action	
	IPSEC ALG	Port Forwarding	Dynamic		
	First Port Triggering Servic	e Trigger Ports	Dynamic		
	Add				
			Close		
http://10.16.90.10:2420/htmlV/welco	omeMain.htm				🥑 Internet

### 15.3.3.4 Deleting a Port Forwarding or Port Triggering Service

If you have created a port forwarding or port triggering service and have added it to your Router's list of active services, at the **Port Forwarding** screen you can do one of the following:

- Click the delete icon 🛱 adjacent to the service you want to delete.
- Click the details icon adjacent to the service you want to view.



User Guide

### 15.4 DMZ Host—Single IP Address Passthrough

In the **Firewall Settings** screen, select **DMZ Host** from the submenu options displayed at the left of the screen. A warning screen will display the following message:

Any changes made in this section may affect your device's performance and configuration. Do you want to proceed?

Click Yes to proceed.

	101	0.0					
	Main	Wireless Settings	My Network	Firewall Settings	Advanced	System Monitoring	
Main			Any changes made in thi	Warning! s section may affect your r Do you want to pr	l devices performance and co oceed? No	nfiguration.	

### **15.4.1 Enabling DMZ Host**

If you clicked **Yes**, in the preceding warning screen, the following **DMZ Host** screen will be displayed. The demilitarized zone (DMZ) feature allows you to select one device on the LAN that will share the WAN-assigned IP address. By enabling DMZ, the selected device becomes visible on the Internet. Network Address Translation (NAT) and Firewall rules do not apply to the device configured for DMZ. If you are using Bridge protocol, you will not be able to configure DMZ Host in the Router.

### **IMPORTANT:**

- 1. Before you configure DMZ Host, configure your PC settings to obtain an IP address from VersaLink automatically. If needed, refer to your computer's Windows help screen for instructions.
- 2. If you have previously enabled Public LAN, you will need to disable Public LAN and enable the DHCP for Private LAN and the Private LAN settings before you configure DMZ Host.
- 3. DMZ Host and Static NAT are mutually exclusive features. Before you enable DMZ Host, confirm that Static NAT is disabled. If needed, refer to section 15.6.2 for details on disabling Static NAT.



User Guide

To configure DMZ Host, in the **DMZ Host** screen, select a device from the drop-down menu. The selected device will share your WAN IP address. Next, click **Enable** to allow the setting to take effect.



If you clicked **Enable** in the preceding screen, the following pop-up screen will appear. The Router must be reset to allow the new configuration to take effect. Click **OK** to continue.





User Guide

If you clicked **OK**, the following screen will appear. After a brief delay, the home page will be displayed. Confirm that you have a DSL link and that your PPP Status displays **UP**. (If necessary, click the **Connect** button to establish a PPP session).

Resetting Modem - Microsoft Internet Explorer		
File Edit View Favorites Tools Help		
veri on		
	Resetting Modem Please Wait	
	The modem is resetting in order for	
	Your page will be reloaded shortly.	-

To confirm that DMZ Host has been enabled, select **Firewall Settings** in the top navigational menu, and then click **DMZ Host** in the submenu options at the left of the screen. Next, click **Yes** in the warning screen. The following **DMZ Host** screen will be displayed. This screen shows that DMZ Host is currently enabled for the selected device.



IMPORTANT: After you enable DMZ Host, you will need to reboot your computer.



User Guide

## 15.4.2 Disabling DMZ Host

To disable DMZ Host (if it has been previously enabled), click **Disable** in the DMZ Host screen.



If you clicked **Disable**, the following screen will be displayed. The Router must be reset to allow the new configuration to take effect. Click **OK** to continue.





User Guide

If you clicked **OK**, the following pop-up screen will appear. After a brief delay, the home page will be displayed. Confirm that you have a DSL link and that your PPP Status displays **UP**. (If necessary, click the **Connect** button to establish a PPP session).

🖉 Verizon - Windows Internet Explorer		
د الله http://192.168.1.1/htmlV/reset.asp?restartSelected=TRUE	🖌 🗲 🗙 Live Search	P •
🔶 🏘 🍘 Verizon		🔐 Home 🔹 🎽
verizon		
Resetting Modem Please Wait		
The modem is resetting in order for the requested changes to take effect.		
Your page will be reloaded shortly.		

**IMPORTANT:** After you disable DMZ Host, you will need to reboot your computer.



User Guide

### 15.5 Remote Administration

In the **Firewall Settings** screen, select **Remote Administration** from the submenu options displayed at the left of the screen. A warning screen will display the following message:

Any changes made in this section may affect your device's performance and configuration. Do you want to proceed?

Click Yes to proceed.

ersaLink Wireless Gate	way - Microsoft Internet	Explorer				l.
1/01	ri on					
		<b>1</b>	112	M		
Main	Wireless	My Network	Firewall	Advanced	System	
			occurgs		nomoring	
Main			Warning!!			
		Any changes made in this	s section may affect your c	levices performance and co	onfiguration.	
			Do you want to pr	oceed?		
			Yes	Nó		

If you clicked **Yes** in the warning screen, the following **Remote Administration** screen will appear. Follow the steps below to configure Remote Administration in your Router.

**NOTE:** The User Name and Password should be at least 4 characters long and should not exceed 32 characters. Do not type a blank space or asterisks. The user name and password are case sensitive.

- 1. Type the administrator's User Name. (By default **admin** appears in this field; however, you can change this value, if desired).
- 2. Type the administrator's Password.
- 3. Enter the number of minutes after which you want remote access to time out.
- 4. Click the Enable Remote Access box (a check mark will appear in the box).
- 5. Click **Apply** to allow the settings to take effect.



User Guide

Ve	ri <mark>, on</mark>					
Main	Wireless Settings	My Network	Firewall Settings	Advanced	System Monitoring	
Main						
General			Remote Administ	ration		
Port Forwarding			Attention	1		
DMZ Host		With Remote Administ	ration enabled, your net	work will be at risk fron	n outside	
Remote Administratio	on		attacks.			
Static NAT						
Security Log		Remote Acc	cess is currently Enabled	l, Timeout is Disabled		
		User Name	admin			
		Password				
		Timeout	20			
		Disable Timeout				
		Enable Remote Access				
		URL:	http://10.16.90.10:2420			
			Apply Can	cel		
						_

Remote Administration			
User Name	Enter the user name in this field.		
Password	Enter your password in this field.		
Timeout	Default = 20 minutes		
	Enter the number of minutes after which remote access will be deactivated. (It will		
	also be deactivated if the Router is reset to factory defaults).		
Disable Timeout	Click this box (a check mark will appear) to activate the Disable Timeout feature.		
	This means that once you enable Remote Access, it will remain on until you reset		
	the Router to factory defaults. This function overrides any timeout values.		
	Deselect the box to deactivate this feature.		
Enable Remote Access	Click this box (a check mark will appear) to enable Remote Access.		
	Deselect the box to disable this feature.		
Remote URL	Displays the URL of the remote management device (VersaLink).		



User Guide

The following screen shows a check mark in the **Enable Remote Access** and **Disable Timeout** check boxes. The following message is displayed:

# Remote access is currently enabled. After 20 minutes of inactivity, or on reboot, remote access will be automatically disabled.

After 20 minutes of inactivity or on reboot, Remote Access will be automatically disabled. To disable Remote Access, click the **Enable Remote Access** box to clear the check mark. Then click **Apply** to allow the change to take effect.

http://10.16.90.10:2420 - Elle Edit <u>V</u> iew F <u>a</u> vorites <u>I</u>	Verizon - Microsoft Int Lools Help	ernet Explorer				-0
ver	ri <mark>zon</mark>					
Main	Wireless Settings	My Network	Firewall Settings	Advanced	System Monitoring	
Main General			Remote Adminis	tration		
Port Forwarding DMZ Host Remote Administration		With Remote Administr	Attention ation enabled, your ne attacks.	<b>n !</b> atwork will be at risk fror	n outside	
Static NAT Security Log		Remote Acc	ess is currently Enable	ed, Timeout is Disabled		
		User Name	admin	]		
		Password	••••	]		
		Timeout	20			
		Disable Timeout				
		Enable Remote Access				
		URL:	http://10.16.90.10:2420			
			Apply Ca	ncel		